A MORE ACCURATE INQUIRY

CONCERNING THE REMAINDERS LEFT BY THE DIVISION OF SQUARES OR

OF HIGHER POWERS BY PRIME NUMBERS

Opuscula analytica 1, 1783, p. 121-156
[E554]

1. If a square number *aa* may be divided by a prime number p , the remainder [or residue] may be indicated by the letter α ; and in a similar manner the remainders in the division of the squares *bb, cc, dd* etc. will be indicated by the letters β, γ, δ etc. by me.

2. Therefore there will be $\alpha = aa - np$, because the remainder α is produced, if a multiple of the number p may be taken from the square *aa* and that shall be a maximum, so that the remainder α from that same divisor may be returned less than p. But nothing stands in the way, why a greater divisor *np* may not be taken for the square *aa,* so that it will produce a negative remainder α , and thus its value can be expressed less than $\frac{1}{2}p$.

3. Therefore the same remainder α can be shown in many ways, because all these forms are composed in the same way $\alpha \pm mp$. Thence it is evident, the remainder arising from the division of the square aa by the number p may be said to be either α , $\alpha \pm p$, or $\alpha \pm mp$, with the letter m denoting some whole number.

4. But innumerable squares *aa* divided by the number p leave the same remainder α, which are all found readily from the one known *aa* . It is clear the whole of these squares to be contained in this form $(a \pm mp)^2$, or $(mp \pm a)^2$, and thus it is to be noted that the remainder from the minimum of these forms suffices, the root of which does not exceed $\frac{1}{2}p$; evidently all these squares $(mp \pm a)^2$ are considered to be of the same nature, with respect to the number p.

5. Thus the remainders themselves will themselves be obtained, arising from the squares put in place following the natural order, on dividing by p :

Squares	1^2,	2^2,	3^2,	4^2,	……	$(p-4)^2$,	$(p-3)^2$,	$(p-2)^2$,	$(p-1)^2$,				
Remainders	1,	4,	9,	16,	……	16,	9,	4,	1.				

Therefore the individual remainders for the squares continued to $(p-1)^2$ occur twice; and because p is a prime number, the number of these is even and the two middle squares $\left(\frac{p-1}{2}\right)^2$ and $\left(\frac{p+1}{2}\right)^2$, will give the same remainder $\frac{pp-2p+1}{4}$.

6. Therefore all the remainders, which indeed are able to come about from the division of the number of squares by the prime number *p*, arise from these squares :

$$\text{Squares:} \quad 1^2, 2^2, 3^2, 4^2, \quad \cdots\cdots \quad \left(\tfrac{p-1}{2}\right)^2,$$
$$\text{Remainders:} \quad 1, \quad 4, \quad 9, \quad 16, \quad \cdots\cdots \quad \tfrac{pp-2p+1}{4}.$$

the number of which is $= \frac{p-1}{2}$. Therefore nor do all the numbers smaller than the divisor *p*, the number of which is $p-1$, occur among the remainders, thence moreover certainly half of these is excluded.

7. But with the squares continued to $\left(\frac{p-1}{2}\right)^2$ the remainders thence arising are all different; nor indeed can any remainder occur twice as far as to this term, if indeed the divisor *p* shall be a prime number. For indeed the two squares *aa* and *bb,* with neither square exceeding $\left(\frac{p-1}{2}\right)^2$, cannot give the same remainder *r ,* and thus the difference of these $aa-bb$ may be divided either by *p,* $a-b$ or $a+b$. But since neither *a* nor *b* shall exceed $\frac{p-1}{2}$, also the sum $a+b$ shall be less than p, and thus generally it cannot happen, that the sum and much less the difference $a-b$ may be allowed to be divided by the number *p*.

8. Therefore for the proposed prime number *p,* all the remainders are obtained from these squares

$$1^2, 2^2, 3^2, 4^2, \quad \cdots\cdots \quad \left(\tfrac{p-1}{2}\right)^2;$$

since the number of which shall be $= \frac{p-1}{2}$ and all the remainders may differ amongst themselves, of the numbers themselves less than *p*, of which the number is $p-1$, certainly half of which occur between the remainders; thence truly half is excluded and constitute the class of *non-remainders*. Therefore for any prime number *p,* the remainders are required to be distinguished properly from the non-remainders.

9. Indeed if α may occur amongst the remainders, we are able to state that innumerable squares be given, which may be contained in this form $np+\alpha$, and the smallest root of those cannot exceed the number $\frac{p-1}{2}$. But if the number $\mathfrak{A}$ may not be found among the remainders, then we will be able to state that no square number be contained in the form $np+\mathfrak{A}$. But in any case both the number of remainders α, as well as the number of non-remainders $\mathfrak{A}$, is $= \frac{p-1}{2}$.

10. But if the remainders arising from the division of the squares by the prime number p may be set out following this natural order, in the first place the square numbers 1, 4, 9, 16 etc. will occur, which from division by the number p can be rendered as smaller numbers; truly the last of these squares will be $\frac{pp-2p+1}{4}$, from which the number p, will be required to be taken away, as many times as it can be done.

11. Towards recognizing this latter remainder, it will be convenient to consider two cases, just as the prime number p were either of the form $4q+1$ or $4q+3$.

The prime number shall be $p=4q+1$ and thus $\frac{p-1}{2}=2q$ and the final remainder $4qq$, which, by the subtraction of the multiple $qp=4qq+q$, is reduced to $-q$, or to $3q+1$.

Truly the other case, $p=4q+3$ or $\frac{p-1}{2}=2q+1$, the final remainder $4qq+4q+1$, with the removal of the multiple $qp=4qq+3q$, is reduced to $q+1$.

12. The penultimate remainder arising from the square $\left(\frac{p-3}{2}\right)^2$ is found in a similar manner :

for the case $p=4q+1: 4qq-4q+1$, or $-5q+1$, or $-q+2$,
for the case $p=4q+3: 4qq$, $-3q$, or $q+3$.

But the next preceding remainder, thus arising from $\left(\frac{p-5}{2}\right)^2$:

for the case $p=4q+1: 4qq-8q+4$, or $-9q+4$, or $-q+6$,
for the case $p=4q+3: 4qq-4q+1$ or $-7q+1$, or $q+7$.

So that truly for the square before the last mentioned above , in this manner, the remainders will be :

for the case $p=4q+1: 4qq-12q+9$, or $-13q+9$, or $-q+12$,
for the case $p=4q+3: 4qq-8q+4$, or $-11q+4$, or $q+13$.

13. Therefore these two cases will be had with the remainders requiring to be identified in the following manner.

In the case $p=4q+1$:

The squares	$1,$	$2^2,$	$3^2,$	$4^2,$	$\cdots$	$(2q-3)^2,$	$(2q-2)^2,$	$(2q-1)^2,$	$(2q)^2,$
The remainders	$1,$	$4,$	$9,$	$16,$	$\cdots$	$-q+12,$	$-q+6,$	$-q+2,$	$-q$
					or	$3q+13,$	$3q+7,$	$3q+3,$	$3q+1.$

In the case $p = 4q + 3$:

The squares	$1,$	$2^2,$	$3^2,$	$4^2,$	$\cdots$	$(2q-2)^2,$	$(2q-1)^2,$	$(2q)^2,$	$(2q+1)^2,$
The remainders	$1,$	$4,$	$9,$	$16,$	$\cdots$	$q+13,$	$q+7,$	$q+3,$	$q+1.$

Clearly in the former case, in general, the remainders $-q+nn+n$ or $3q+nn+n+1$ occur, but truly in the latter, $q+nn+n+1$.

14. So that this order of the remainders may be seen more clearly, I shall set out several examples requiring to be examined, and indeed the first for prime numbers of the form $p = 4q+1$.

$p = 5 \begin{cases} 1, & 2^2, \\ q = 1 \\ 1, & 4 \end{cases}$

or $1, -1$

$p = 13 \begin{cases} 1, & 2^2, & 3^2, & 4^2, & 5^2, & 6^2 \\ q = 3 \\ 1, & 4, & 9, & 3, & 12, & 10 \end{cases}$

or $1, 4, -4, \quad 3, -1, -3$

$p = 17 \begin{cases} 1, & 2^2, & 3^2, & 4^2, & 5^2, & 6^2, & 7^2, & 8^2 \\ q = 4 \\ 1, & 4, & 9, & 16, & 8, & 2, & 15, & 13 \end{cases}$

or $1, 4, -8, -1, 8, 2, -2, -4$

$p = 29 \begin{cases} 1, & 2^2, & 3^2, & 4^2, & 5^2, & 6^2, & 7^2, & 8^2, & 9^2, & 10^2, & 11^2, & 12^2, & 13^2, & 14^2 \\ q = 7 \\ 1, & 4, & 9, & 16, & 25, & 7, & 20, & 6, & 23, & 13, & 5, & 28, & 24, & 22 \end{cases}$

or $1, 4, 9, -13, -4, 7, -9, 6, -6, 13, 5, -1, -5, -7$

$p = 37 \begin{cases} 1, & 2^2, & 3^2, & 4^2, & 5^2, & 6^2, & 7^2, & 8^2, & 9^2, & 10^2, & 11^2, & 12^2, & 13^2, & 14^2, & 15^2, & 16^2, & 17^2, & 18^2 \\ q = 9 \\ 1, & 4, & 9, & 16, & 25, & 36, & 12, & 27, & 7, & 26, & 10, & 33, & 21, & 11, & 3, & 34, & 30, & 28 \end{cases}$

or $1, 4, 9, 16, -12, -1, 12, -10, 7, -11, 10, -4, -16, 11, 3, -3, -7, -9$

$p = 41 \begin{cases} 1, & 2^2, & 3^2, & 4^2, & 5^2, & 6^2, & 7^2, & 8^2, & 9^2, & 10^2, & 11^2, & 12^2, & 13^2, & 14^2, & 15^2, & 16^2, & 17^2, & 18^2, & 19^2, & 20^2 \\ q = 10 \\ 1, & 4, & 9, & 16, & 25, & 36, & 8, & 23, & 40, & 18, & 39, & 21, & 5, & 32, & 20, & 10, & 2, & 37, & 33, & 31 \end{cases}$

or $1, 4, 9, 16, -16, -5, 8, -18, -1, 18, -2, -20, 5, -9, 20, 10, 2, -4, -8, -10$

Where it may be noted for the remainders on being reduced to the minimum form by subtraction, the individual numbers to occur twice, evidently positive and negative.

15. The following examples pertain to prime numbers of the form $p = 4q + 3$.

$$\begin{array}{l} p = 3 \\ q = 0 \end{array} \left\{ \begin{array}{l} 1 \\ 1 \end{array} \right.$$

$$\begin{array}{l} p = 7 \\ q = 1 \end{array} \left\{ \begin{array}{l} 1,\ 2^2,\ 3^2 \\ 1,\ 4,\ \ 2, \end{array} \right.$$

or $\quad 1, -3,\ 2$

$$\begin{array}{l} p = 11 \\ q = \ 2 \end{array} \left\{ \begin{array}{l} 1,\ 2^2,\ 3^2,\ 4^2,\ 5^2 \\ 1,\ 4,\ \ 9,\ \ \ 5,\ \ 3 \end{array} \right.$$

or $\quad 1,\ 4, -2,\ \ \ 5,\ \ 3$

$$\begin{array}{l} p = 19 \\ q = \ 4 \end{array} \left\{ \begin{array}{l} 1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ 8^2,\ 9^2 \\ 1,\ 4,\ \ 9,\ 16,\ \ 6,\ \ 17,\ 11,\ \ 7,\ \ 5 \end{array} \right.$$

or $\quad 1,\ 4,\ \ 9,\ -3,\ \ 6,\ -2,\ -8,\ 7,\ \ 5$

$$\begin{array}{l} p = 23 \\ q = \ 7 \end{array} \left\{ \begin{array}{l} 1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ \ 8^2,\ 9^2,\ 10^2,\ 11^2 \\ 1,\ 4,\ \ 9,\ 16,\ \ 2,\ \ 13,\ \ \ 3,\ \ 18,\ 12,\ 8,\ \ \ 6 \end{array} \right.$$

or $\quad 1,\ 4,\ \ 9,\ -7,\ 2, -10,\ \ \ 3,\ -5, -11,\ 8,\ \ 6$

$$\begin{array}{l} p = 31 \\ q = \ 5 \end{array} \left\{ \begin{array}{l} 1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ \ 8^2,\ 9^2,\ 10^2,\ 11^2,\ 12^2,\ 13^2,\ 14^2,\ 15^2 \\ 1,\ 4,\ \ 9,\ 16,\ \ 25,\ 5,\ \ 18,\ 2,\ \ \ 19,\ \ 7,\ \ 20,\ \ 33,\ \ 14,\ \ \ 10,\ \ \ 8, \end{array} \right.$$

or $\quad 1,\ 4,\ \ 9, -15,\ \ -6,\ \ 5, -13,\ \ 2,\ -12,\ \ 7,\ -11, -16,\ \ \ 14,\ \ \ 10,\ \ \ 8,$

$$\begin{array}{l} p = 43 \\ q = \ 10 \end{array} \left\{ \begin{array}{l} 1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ \ 8^2,\ 9^2,\ 10^2,\ 11^2,\ 12^2,\ 13^2,\ 14^2,\ 15^2,\ 16^2,\ 17^2,\ 18^2,\ 19^2,\ \ 20^2,\ \ 21^2 \\ 1,\ 4,\ \ 9,\ 16,\ \ 25,\ 36,\ 6,\ 21,\ 38,\ \ 14,\ \ \ 35,\ \ 15,\ \ \ 40,\ \ \ \ 4,\ 10,\ \ 41,\ \ 31,\ \ \ 23,\ 17,\ \ 13,\ \ \ 11 \end{array} \right.$$

or $\quad 1,\ 4,\ \ 9,\ \ 16, -18, -7,\ \ 6,\ \ 21,\ -5,\ \ 14,\ \ -8,\ \ 15,\ \ -3,\ \ -19,\ 10,\ \ -2, -12,\ \ -20,\ \ 17,\ \ 13,\ \ \ 11$

In accordance with the same remainders reduced to a minimum form plainly all the numbers from one to $2q + 1$ occur, some with the sign of position, others affected by a negative sign. Truly it is required to show these observed properties.

16. Now above, [E552, Theorem II], I have shown, if the numbers α and β occur among the remainders arising from the division of the squares by some number *p,* in the same place also the product $\alpha\beta$ to be found and hence also this form $\alpha^m \beta^n$, extended more widely. For these remainders arise from the squares *aa* and *bb,* thus so that there shall be :

$$aa = mp + \alpha \text{ and } bb = np + \beta,$$

and it is evident from the product of these squares :

$$aabb = mnpp + (m\beta + n\alpha)p + \alpha\beta,$$

of which the form is $Mp + \alpha\beta$, the remainder $\alpha\beta$ having arisen; and in a similar manner the remainder $\alpha^m\beta^n$ or $a^m\beta^n - Mp$ comes from the square $a^{2m}b^{2n}$, so that it may be reduced to the minimum form. It will be agreed also to be noted this same remainder $\alpha^m\beta^n$ has arisen from all these squares $(a^mb^n \pm Np)^2$ or $(Np \pm a^mb^n)^2$ and thus from the square, of which the side $a^mb^n - Np$ or $Np - a^mb^n$ will be smaller than $\frac{1}{2}p$.

17. The letters

$$a,\ b,\ c,\ d,...l$$

may denote all the numbers of the divisor p less than $\frac{1}{2}p$, of which the amount is $= \frac{p-1}{2}$, and there shall be the remainders

$$\alpha,\ \beta,\ \gamma,\ \delta,...\lambda$$

arising from the squares of these

$$a^2,\ b^2,\ c^2,\ d^2,...l^2$$

left from the division by the number p , the number of which likewise is $= \frac{p-1}{2}$, thus so that from all the smaller numbers from the divisor p , of which the amount is $p-1$, just as many may be excluded from the order of the remainders, which I will indicate by the gothic script

$$\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \ldots \mathfrak{L}.$$

Therefore it is especially noteworthy in the order of the remainders $\alpha,\ \beta,\ \gamma,\ \delta,...\lambda$, even if the number of these is only $= \frac{p-1}{2}$, yet all of the same products from two and more and also all the individual powers occur, if indeed thence by being taken away, as often as that can be done, they may recall the divisor p to the minimal form.

18. So that this may be illustrated further, it shall be required to take into account how all the numbers in just as many kinds of each divisor p are to be distributed; evidently in the account of the divisor 2 two kinds of numbers contained of even and odd formulas $2x$ and $2x+1$. But the divisor 3 presents three kinds of numbers $3x,\ 3x+1$ and $3x+2$; and the divisor 4 these four $4x,\ 4x+1,\ 4x+2$ and $4x+3$, which different kinds are

accustomed to be distinguished with care in the theory of numbers. Therefore in a similar manner in the account of each divisor *p* these diverse kinds of numbers are established

$$px,\ px+1, px+2, px+3,\ ...px+p-1,$$

the number of which is *p.* Therefore with the first kind *px* omitted, with a multiple of the divisor *p* contained, the number of divisors of the rest is $p-1$, and if *p* were a prime number, it is agreed these kinds be divided into two classes with each containing $\frac{p-1}{2}$ kinds:

$$px+\alpha,\ px+\beta,\ px+\gamma,\ px+\delta,...px+\lambda,$$
$$px+\mathfrak{A}, px+\mathfrak{B}, px+\mathfrak{C}, px+\mathfrak{D},...px+\mathfrak{L},$$

thus so that all the square numbers may be contained in the first class, truly the latter class shall be completely against nature of the squares.

19. Therefore for any prime divisor *p* with these two classes in place, each of which may will contain $\frac{p-1}{2}$ kinds of remainders, and which both taken together plainly contain all the numbers with the exception of multiples of *p* itself, certainly of which it is a judgment at once, all the numbers in the first class make use of this property, in order that the product from two may be contained in the same class, in which therefore likewise not only the powers of any individual members, but also the products from two or several of these powers occur. Therefore the first class, that I call the class of the remainders, is determined by the $\alpha,\ \beta,\ \gamma,\ \delta,...\lambda$, while the other class of the non-remainders, is defined by the numbers $\mathfrak{A},\mathfrak{B},\mathfrak{C},\mathfrak{D},\ldots\mathfrak{L}$.

20. From which also I have shown, if in the class of remainders the two numbers *r* and *rs* occur, of which *r* shall be a factor of *rs*, then also another factor of this is to be found in the same class. For since two squares may be given *aa* et *bb,* so that the forms $aa-r$ and $bb-rs$ shall be divisible by the prime number *p* with the numbers *a* and *b* themselves smaller than *p* , also the form $aas-rs$ is divisible by *p* and hence also the differences $bb-aas$ and $(b+np)^2-aas$. But since *a* and *b* shall be smaller than *p,* thus it is allowed always to assume *n*, so that there may become $b + np = ma.$ From which such a form $mmaa-aas$ will be given divisible by *p* and thus also this $mm-s$, so that there shall be $s=mm-np$ and therefore the number *s* may be found amongst the remainders. Hence if follows, if *r* were a remainder, but *s* a non-remainder, then the product *rs* surely becomes a non-remainder; or the products made from any remainder by non-remainder, such as $\alpha\mathfrak{A},\alpha\mathfrak{B},\beta\mathfrak{A}$, are found amongst the non-remainders.

21. Therefore if $\mathfrak{A}$ were a non-remainder, all these products $\alpha\mathfrak{A},\ \beta\mathfrak{A},\ \gamma\mathfrak{A},\ \delta\mathfrak{A},...\lambda\mathfrak{A}$

will be non-remainders; which since they shall be different from each other also by a reduction made to the simplest form with the number of these made $= \frac{p-1}{2}$, therefore all the non-remainders are held in these. From which now it is seen the product from two non-remainders, such as $\alpha\beta\mathfrak{AA}$, is required to be referred to the class of remainders, since $\alpha\beta$ is a remainder and $\mathfrak{AA}$ as a square number itself occurs amongst the remainders. Therefore in a similar manner it is apparent the product from three non-remainders to be used, $\mathfrak{ABC}$, again falls in the class of non-remainders, truly the products from four will be found among the same remainders, and thus so on.

22. Truly I observe besides also a new remainder to arise from the two given remainders α and β by division and the fraction $\frac{\alpha}{\beta}$ between the remainders is required to be examined. Indeed even if the fractions arising directly from this ratio are excluded, yet, because the number α may be considered to be equivalent to this general form $\alpha + np$ containing all kinds, each number thus may be allowed to be taken, so that $\frac{\alpha+np}{\beta}$ becomes a whole number integer, from which pronouncement it is required to be understood, how evidently it may be found between the remainders. Hence therefore all the terms of this geometric progression

$$\alpha,\ \beta,\ \frac{\beta^2}{\alpha},\ \frac{\beta^3}{\alpha^2},\ \frac{\beta^4}{\alpha^3},\ \text{etc.}$$

may be contained in the class of remainders from the two remainders α and β made continuously, evidently if the individual terms may be recalled to whole number form. So that if indeed the fraction $\frac{\beta}{\alpha}$ may be equivalent to the whole number *r,* the following whole numbers are obtained at once

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\ \beta r^4\ \text{etc.},$$

which are unable to produce more diverse numbers than $\frac{p-1}{2}$ on being reduced to the standard form.

23. Therefore we will consider this geometric progression

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\ \beta r^4\ \text{etc.},$$

and since all the terms are unable to be different, these terms βr^m and βr^{m+n} divided by p leave the same remainder, thus so that the difference $\beta r^{m+n} - \beta r^m$ and therefore $r^n - 1$ may become divisible by p. Therefore moreover also the terms β and βr^n and also

α and βr^{n-1} will agree in the account of the remainders; from which it is apparent more different remainders cannot be produced, than which arise from these initial terms

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\cdots \beta r^{n-2},$$

because from the following $\beta r^{n-1},\ \beta r^n,\ \beta r^{n+1}$ etc. the same remainders recur in the same order ; therefore the number of which remainders, if indeed they were different, the number cannot be greater than $\frac{p-1}{2}$, which arises, if r^n shall be the smallest power of $r,$ which diminished by one may be allowed to be divided by p. Hence it is apparent the number n certainly cannot exceed $\frac{p-1}{2}$; and if there were $n=\frac{p-1}{2}$, clearly all the remainders will be obtained.

24. Nevertheless, if not all the remainders may be produced from the terms $\alpha,\ \beta,\ \beta r,\ \beta r^2,\cdots \beta r^{n-2},$ but certain ones may be omitted, it is easily shown how many are present, for the smallest total omitted. For if the remainder γ may not occur among these, which also can be represented by $\alpha\delta$, since $\gamma+mp$ can always be recalled to the form $\alpha\delta$, then also neither $\beta\delta$, nor $\beta\delta r$, $\beta\delta r^2$ etc. will be found among these remainders ; which since they are different, with the one excluded likewise n are excluded, from which $2n$ cannot surpass the number of all the remainders, $\frac{p-1}{2}$. Therefore there will be either $2n=\frac{p-1}{2}$ or $2n<\frac{p-1}{2}$ and for the latter case at this point anew the remainders are excluded to the minimum n. Whereby since the terms of the geometric progression $\alpha,\ \beta,\ \beta r,\ \beta r^2,\cdots \beta r^{n-2},$ the number of which is $n,$ or all the remainders arising from squares may be contained, the number of which is $=\frac{p-1}{2}$, thence either the number excluded shall be $=n$, $=2n$, or $=3n$ etc., it is evident by necessity that the number n must be a certain minimum part of $\frac{p-1}{2}$ itself, and thus the minimum exponent $n,$ by which the power r^n diminished by one may be rendered divisible by p, or by the number $\frac{p-1}{2}$ itself , or to be equal to some other part of the same .

25. But if there shall be $n=\frac{p-1}{2}$, or it may be equal to some other part, the form $r^{\frac{1}{2}(p-1)}-1$ is allowed always to be divided by the prime number $p.$ We may put $p=2q+1$, so that there shall become $\frac{p-1}{2}=q$; and if from any two remainders of the squares α and β by taking $r=\frac{\beta+np}{\alpha}$, this geometric progression may be formed :

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\cdots \beta r^{q-2}$$

with the number of terms present $=q$, hence then either all the remainders of the squares will result $\alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\cdots\lambda$ or only half of these, or the third or fourth part, or some other amount ; and likewise it is observed, how many different ones will have emerged from the beginning, the same hence are going to be repeated continually in the same order. But the following terms $\beta r^{n-1},\ \beta r^{n},\ \beta r^{n+1}$ etc. always will produce the same remainders $a,\ \beta,\ \beta r$ etc., which they had in the beginning.

26. Therefore as often as q is a prime number present with $p=2q+1$, then the geometric progression formed from any remainders α and β of two squares and continued to q terms

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\cdots\beta r^{q-2}$$

plainly will show all the remainders of the squares with none excluded nor repeated. Therefore all the remaining remainders $\gamma,\ \delta,\ \varepsilon,\cdots\lambda$ will agree with some such term βr^n, so that there shall be $n<q-1$. But if the number q were composite, by putting $q=mn$ and $p=2mn+1$, then it can eventuate, so that not all the remainders of the squares thus may be produced, but only some part of q of this kind, such as its nature allows. But if as it usually happens, the whole geometric progression consisting of q terms can be separated at once into two or more parts, in which the same remainders recur.

27. Since there shall be $\frac{\beta}{\alpha}=r$ and thus $\beta=\alpha r$, our geometric progression may be expressed more clearly in this manner

$$\alpha,\ \alpha r,\ \alpha r^2,\ \beta r^3,\cdots\alpha r^{q-1}$$

because all the terms of which have been multiplied by α, thus with this common factor omitted the progression thus can be shown more simply. Clearly with the prime divisor proposed $p=2q+1$ if some remainder were α, the individual terms of this progression the number of which is $=q$, are found among the remainders of the squares, and if all may pertain to diverse kinds, also they will fill up the whole class of remainders. But it can happen, as we have seen, that not all the remainders may be produced in this manner, but only some aliquot part of the whole class, while the same after a certain period are repeated again, hence truly the remaining parts evidently are excluded.

28. But if all the remainders of the squares may be generated from this geometrical progression or only a certain aliquot part, those, which are contained in the terms of this progression, as have been endowed with the signified properties, so that there is a need for this to be set out more accurately. Therefore I note in the first place, if this geometrical progression may be continued further, the following terms $\alpha^q,\ \alpha^{q+1},\ \alpha^{q+2}$

etc. to be equivalent to the first 1, α, α^2 etc., therefore since a^{q-1} certainly can be divided by the prime divisor $p = 2q+1$. Therefore with the following term α^q being added equivalent to unity, thus so that we may have

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\cdots\alpha^{q-3},\ \alpha^{q-2},\ \alpha^{q-1},1,$$

because the product from the first term into the last is $=1$, from the nature of the geometrical progression , from the second α by the second last α^{q-1}, likewise from the third α^2 by the third from last α^{q-2}, and in general from two equidistant from the ends α^m and α^{q-m} to be reduced to unity.

29. Therefore with some remainder α given among the remainders one may be found β, thus so that the product $\alpha\beta$ may be equivalent to unity or there shall be $\beta = \frac{1+np}{\alpha}$, from which that is found easily. Therefore these two remainders, α and β , may be gathered together with such a link between them, I will call these *reciprocals* [*i.e. associated or united*]; from which each two terms supply the needs of the two reciprocal terms of this kind, equidistant from the ends of the above geometric progression. Evidently the second to last term α^{q-1} itself is equivalent to β, the one preceding α^{q-2} to β^2 itself, and thus henceforth; from which if the reciprocal [or associated] terms may be written in this manner

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\cdots\alpha^{q-3},\ \alpha^{q-2},\ \alpha^{q-1},\ 1,$$
$$1,\ \beta,\ \beta^2,\ \beta^3,\cdots\beta^{q-3},\ \beta^{q-2},\ \beta^{q-1},\ 1,$$

the lower series agrees with the upper written backwards. But always the reciprocal of the remainder of one is one also.

30. The consideration of these reciprocal remainders reveals a way for us to uncover significant properties. For since on putting the prime divisor $p = 2q+1$, the number of all the divisors shall be q, of which any besides unity comes together with its reciprocal, with unity excluded from the remainders, the number of which is $= q-1$, following this association, they can be distributed in pairs with two reciprocals united together in turn. Hence if $q-1$ were an odd number and therefore q even, it is necessary, that in this distribution the same remainder, for example δ, may occur twice. Truly the same remainder δ cannot be associated with two different remainders ; if indeed there were $\alpha\delta = 1$ and $\beta\delta = 1$, the remainders α and β cannot differ. Whereby no other remains, except that the same remainder δ may be associated with that and therefore there shall be $\delta\delta = 1$, from which there becomes either $\delta = 1$ or $\delta = -1$; but because unity now has been put aside, it is necessary in this case, where q is an even number, -1 or $p-1$ to be found among the remainders.

31. Behold therefore an outstanding demonstration of the above truth now observed, so that, if the prime divisor shall be $p = 4m+1$ and thus $q = 2m$, by necessity -1 occurs amongst the remainders or the square *aa* may be able to be shown always, so that $aa+1$ shall be able to be divided by that prime number $p = 4m+1$. Hence likewise it is apparent, if the number α shall be among the remainders, in that place also the product $-1\cdot\alpha$, evidently $-\alpha$, to occur and hence all the remainders present both positive as well as negative to be reduced to the minimum form, generally as is seen to arise in the examples in § 14. Truly likewise it is apparent, if there were $p = 4m+3$ and thus the number of remainders odd, as -1 is not to be found there, because the individual remainders each may occur with the $+$ and $-$ sign, and thus the number of these cannot be odd [see Th. 4 of E552]. From which it follows no sum of two squares can be divided for a prime number of this kind $p = 4m+3$.

32. But for prime divisors of the form $p = 4m+3$, if the square *aa* may give the remainder α, always another will give the square *bb* bearing the remainder $-\alpha$; and thus the sum of the squares of these $aa+bb$ will be divisible by that prime number, thus so that neither *a* nor *b* may exceed $2m$. Therefore there will be a need for these cases with the sign differences to be shown together and likewise the squares, from which they arise, to be written :

$$p=5\begin{cases}+1 & 1^2\\ -1 & 2^2\end{cases}\qquad p=13\begin{cases}+1,\ +4,\ +3 & 1^2\ \ 2^2\ \ 4^2\\ -1,\ -4,\ -3 & 5^2\ \ 3^2\ \ 6^2\end{cases}\qquad p=17\begin{cases}+1,\ +2,\ +4,\ +8 & 1^2\ \ 6^2\ \ 2^2\ \ 5^2\\ -1,\ -2,\ -4,\ -8 & 4^2\ \ 7^2\ \ 8^2\ \ 3^2\end{cases}$$

$$p=29\begin{cases}+1,\ +4,\ +5,\ +6\ \ +7,\ +9,\ +13, & 1^2\ \ 2^2\ \ 11^2\ \ 8^2\ \ 6^2\ \ 3^2\ \ 10^2\\ -1,\ -4,\ -5,\ -6\ \ -7,\ -9,\ -13, & 12^2\ \ 5^2\ \ 13^2\ \ 9^2\ \ 14^2\ \ 7^2\ \ 4^2\end{cases}$$

$$p=37\begin{cases}+1,\ +3,\ +4,\ +7\ \ +9,\ +10,\ +11,\ +12,\ +16 & 1^2\ \ 15^2\ \ 2^2\ \ 9^2\ \ 3^2\ \ 11^2\ \ 14^2\ \ 7^2\ \ 4^2\\ -1,\ -3,\ -4,\ -7\ \ -9,\ -10,\ -11,\ -12,\ -16 & 6^2\ \ 16^2\ \ 12^2\ \ 17^2\ \ 18^2\ \ 8^2\ \ 10^2\ \ 5^2\ \ 13^2\end{cases}$$

$$p=41\begin{cases}+1,\ +2,\ +4,\ +5\ \ +8,\ +9,\ +10,\ +16,\ +18,\ +20 & 1^2\ \ 17^2\ \ 2^2\ \ 13^2\ \ 7^2\ \ 3^2\ \ 16^2\ \ 4^2\ \ 10^2\ \ 15^2\\ -1,\ -2,\ -4,\ -5\ \ -8,\ -9,\ -10,\ -16,\ -18,\ -20 & 9^2\ \ 11^2\ \ 18^2\ \ 6^2\ \ 19^2\ \ 14^2\ \ 20^2\ \ 5^2\ \ 8^2\ \ 12^2\end{cases}$$

33. Hence it is evident for the prime divisor $p=4m+1$ both the square roots having been able to be assigned in just as many ways, as m contains ones, not exceeding the limit $2m$, the sum of which shall be divisible by the number p. But with these two squares there is no law, by which they may be associated together, and the sum of the others at one time or another is found to be greater or smaller, and the minimum indeed is equal to the number p itself. But whether always the sum of two such squares may be given equal to the divisor p, hence may be seen not to be easy to demonstrate. But since from another source I have shown the sum of two squares not to allow divisors, except those which themselves shall be the sum of two squares, because here it has prevailed always the sums of two squares to be given, which always shall be divisible by the prime number $p=4m+1$, now certainly it may be agreed prime numbers of the form $4m+1$ to be the sum of two squares. But the present supplementary demonstration confirms this wonderfully. Indeed at one time the sum of the squares of this kind to be shown only by many indirect arguments, which shall be divisible by some prime number of the form $4m+1$, because here that has been placed in the light.

34. But with the sum of two squares $aa+bb$ given divisible by the prime number p thence likewise it will be allowed to find other outstanding sums of two squares.

1. If the numbers a and b may have a common divisor, so that there shall be $a=nc$ and $b=nd$, also the sum of the squares $cc+dd$ will be divisible by p.

2. If both the numbers a and b shall be odd and thus $\frac{a+b}{2}$ and $\frac{a-b}{2}$ whole numbers, also the sum of the squares of these will be allowed to be divided by p ; moreover that is half of the preceding.

3. Then truly also these sums of squares $(p-a)^2+(p-b)^2$ or $a^2+(p-b)^2$ will be divisible by p ; from which if the common divisor roots may be drawn out, by that they may be returned to the smaller form.

4. Therefore if both $a=2c+1$ and $b=2d+1$, on account of $p=4m+1$ shall be odd, the sum of these squares $(2m-c)^2+(2m-d)^2$ will be divisible by p ; and if the one be even $a=2c$, the other odd $b=2d+1$, this sum $cc+(2m-d)^2$ will be divisible by p ; and in this way more sums of two squares can be found continually.

35. These will become clearer by example. Therefore with the divisor taken $p=41$, the sum of the two squares shall be found 17^2+11^2 divisible by that, so that there shall be $a=17$ and $b=11$, and by these rules the following values for all a and b may be found :

$$p=41\begin{cases} a=17,24 & 4,\ 4 & 1,40 & 5 \\ b=11,30 & 5,36 & 9,32 & 4 \end{cases}$$

Then truly again from the case, where either of the numbers is $=1$, and some other value thus can be attributed to the other, so that it may remain below $\frac{1}{2}p$. Clearly with the case found, $a=1$ and $b=9$ also satisfies $a=m$ and $b=9m$, where the can be taken in place of b, $9m-np$ or $np-9m$, thus so that b may be expressed less than $\frac{1}{2}p$; and thus all the numbers will be allowed to be accepted for a :

$a=1$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	15	etc.
$b=9$	18	14	5	4	13	19	10	1	8	17	15	6	3	12	20	etc.

Therefore a method is desired among all these two values of the letters a and b, these requiring to be found, the sum of the squares of which shall be a minimum, so that henceforth the sum of the squares may be shown to be a minimum, so that henceforth it may be shown this sum certainly to become equal to the divisor 41 itself; so that indeed it comes about in the case presented, if the values of the letters a and b shall be 4 and 5.

36. But I revert to that disposition of the squares arising from the remainders, by which I have observed this following geometric progression can be put in place. Therefore the prime divisor shall be $p = 2q + 1$ and the remainders thence arising from the squares shall be written in some order:

$$1,\ \alpha,\ \beta,\ \gamma,\ \delta,...\lambda,$$

the number of which is $= q$, and all the following geometric progressions will be continued in these remainders :

$$1,\ \alpha,\ \alpha^2,\ \alpha^3, a^4,\cdots\ \alpha^{q-1}$$
$$1,\ \beta,\ \beta^2,\ \beta^3, \beta^4,\cdots\ \beta^{q-1}$$
$$1,\ \gamma,\ \gamma^2,\ \gamma^3, \gamma^4,\cdots\ \gamma^{q-1},$$
$$1,\ \delta,\ \delta^2,\ \delta^3, \delta^4,\cdots\ \delta^{q-1}$$
$$\text{etc.,}$$

in which all the following terms $\alpha^q,\ \beta^q,\ \gamma^q,\ \delta^q,...\lambda^q$, will be equivalent to one, certainly all of which decreased by one will be divisible by the divisor p . Therefore just as many geometric progressions of this kind can be shown, as there are ones contained in the number q , and in all of these no term will occur, which may not be found among the remainders $1,\ \alpha,\ \beta,\ \gamma,\ \delta,...\lambda$.

37. But it can happen, has §.24 has shown above, that not all of these geometric progressions, even if the number of terms of each shall be $= q$, may give rise to all the remainders, but only either half of these, or a third, or also some other aliquot part ; so that it may pertain for such cases to be considered more carefully.

Therefore I observe initially, if q were a prime number, this cannot come about in use in any way ; for if in a geometrical progression of this kind of the q terms, not all the remainders occur, of these which occur, it is necessary the individual terms occur either twice, three times, or some aliquot number. From which if q is a prime number, any geometric progression includes all the different remainders for the number q. Thus if $p = 11$ and $q = 5$, from the five remainders

$$1,\ 4,\ -2,\ 5,\ 3$$

these four geometric progressions may be formed on starting from unity :

$$\left|\begin{array}{ll} & 1,\ 4,\ 4^2,\ 4^3,\ 4^4 \\ \text{or} & 1,\ 4,\ 5,\ -2,\ \ 3 \end{array}\right| \quad \left|\begin{array}{ll} & 1,\ -2,\ \ 2^2,\ -2^3,\ 2^4 \\ \text{or} & 1,\ -2,\ \ \ 4,\ \ \ 3,\ \ \ 5 \end{array}\right|$$

$$\left|\begin{array}{ll} & 1,\ 5,\ 5^2,\ 5^3,\ 5^4 \\ \text{or} & 1,\ 5,\ 3,\ \ 4,\ -2 \end{array}\right| \quad \left|\begin{array}{ll} & 1,\ \ \ 3,\ \ 3^2,\ 3^2,\ 3^4 \\ \text{or} & 1,\ \ \ 3,\ -2,\ 5,\ 4 \end{array}\right|$$

Where the individual remainders may be changed through all the places except the first.

38. Hence it is evident the remainders can be formed easily from any of these remaining geometric progressions, while from that by a leap jumping across either one, two, or several more terms, terms may be picked out from this numeration, when it will have arrived at the end, starting again from the beginning. Thus if we may take the case, where $p = 23$ and $q = 11$, and the remainders

$$1,\ 4,\ 9,\ -7,\ 2,\ -10,\ 3,\ -5,\ -11,\ 8,\ 6,$$

form a single geometric progression, of which I inscribe the indices for the terms, from which henceforth the rest may be able to be shown more easily by jumps being selected, ten geometric progressions thus will be established:

												Etc.
1.	Indices	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10	0
	Progression	1,	4,	−7,	−5,	3,	−11,	2,	8,	9,	−10,	6	1
2.	Indices	0,	2,	4,	6,	8,	10,	1,	3,	5,	7,	9	0
	Progression	1,	−7,	3,	2,	9,	6,	4,	−5,	−11,	8,	−10	1
3.	Indices	0,	3,	6,	9,	1,	4,	7,	10,	2,	5,	8	0
	Progression	1,	−5,	2,	−10,	4,	3,	8,	6,	−7,	−11,	9	1
4.	Indices	0,	4,	8,	1,	5,	9,	2,	6,	10,	3,	7	0
	Progression	1,	3,	9,	4,	−11,	−10,	−7,	2,	6,	−5,	8	1
5.	Indices	0,	5,	10,	4,	9,	3,	8,	2,	7,	1,	6	0
	Progression	1,	−11,	6,	3,	−10,	−5,	9,	−7,	8,	4,	2	1
6.	Indices	0,	6,	1,	7,	2,	8,	3,	9,	4,	10,	5	0
	Progression	1,	2,	4,	8,	−7,	9,	−5,	−10,	3,	6,	−11	1
7.	Indices	0,	7,	3,	10,	6,	2,	9,	5,	1,	8,	4	0
	Progression	1,	8,	−5,	6,	2,	−7,	−10,	−11,	4,	9,	3	1
8.	Indices	0,	8,	5,	2,	10,	7,	4,	1,	9,	6,	3	0
	Progression	1,	9,	−11,	−7,	6,	8,	3,	4,	−10,	2,	−5	1
9.	Indices	0,	9,	7,	5,	3,	1,	10,	8,	6,	4,	2	0
	Progression	1,	−10,	8,	−11,	−5,	4,	6,	9,	2,	3,	−7	1
10.	Indices	0,	10,	9,	8,	7,	6,	5,	4,	3,	3,	1	0
	Progression	1,	6	−10,	9,	8,	2,	−11,	3,	−5,	−7,	4	1

Clearly the indices to be rising here beyond 11 have been expressed smaller by 11 being subtracted. Here again it is agreed two remainders to be observed, of which the indices together make 11 or in general *q,* to be the link associated with the product of these equivalent to unity. Truly in this case the associated remainders are

$$4,\ -7,\ -5,\ 3,\ -11,$$
$$6,\ -10,\ 9,\ 8,\ 2.$$

39. Now we will consider some cases, in which q is a composite number and initially the double of some prime number. We may begin from the example, where $p = 13$ and $q = 6 = 2 \cdot 3$ and these the remainders :

$$1,\ 4,-4,\ 3,-1,-3,$$

from which these five geometrical progressions may be formed :

$$\begin{aligned}
&\text{I. } 1,\ 4,\ 3,\ -1,\ -4,\ -3,\\
&\text{II. } 1,\ -4,\ 3,\ 1,\ -4,\ 3,\\
&\text{III. } 1,\ 3,\ -4,\ 1,\ 3,\ -4,\\
&\text{IV. } 1,\ -1,\ 1,\ -1,\ 1,\ -1,\\
&\text{V. } 1,\ -3,\ -4,\ -1,\ 3,\ 4.
\end{aligned}$$

Where the first and the fifth contain all the remainders, truly the second and the third of these only the half of these 1, - 4, 3, which are repeated twice with the rest $-1,\ +4,\ -3$ excluded, the fourth truly has only the two $+1$ and -1 repeated three times.

A similar account may be had in the case $p = 29$ and $q = 14 = 2 \cdot 7$, where the remainders are :

$$1,\ 1,\ 4,\ 4,\ 5,\ 5,\ 6,\ 6,\ 7,-7,\ 9,-9,\ 13,-13,$$

from which these geometric progressions are formed :

$$\begin{aligned}
&\left\{\begin{matrix}\text{I.}\\ \text{II.}\end{matrix}\right. \begin{matrix}1, & -1 & 1, & -1, & 1, & -1 & 1, & -1, & 1, & -1, & 1, & -1, & 1, & -1,\\ 1, & 4, & -13, & 6, & -5, & 9, & 7, & -1, & -4, & 13, & -6, & 5, & -9, & 7,\end{matrix}\\
&\left\{\begin{matrix}\text{III.}\\ \text{IV.}\end{matrix}\right. \begin{matrix}1, & -4 & -13, & -6, & -5, & -9, & 7, & 1, & -4, & -13 & -6, & -5, & -9, & 7,\\ 1, & 5, & -4, & 9, & -13, & -7, & -6, & -1, & -5, & 4, & -9, & 13, & 7, & 6,\end{matrix}\\
&\left\{\begin{matrix}\text{V.}\\ \text{VI.}\end{matrix}\right. \begin{matrix}1, & -5, & -4, & -9, & -13, & 7, & -6, & 1, & -5, & -4, & -9, & -13, & 7, & -6,\\ 1, & 6, & 7, & 13, & -9, & 4, & -5, & -1, & -6, & -7, & -13, & 9, & -4, & 5,\end{matrix}\\
&\left\{\begin{matrix}\text{VII.}\\ \text{VIII.}\end{matrix}\right. \begin{matrix}1, & -6, & 7, & -13, & -9, & -4, & -5, & 1, & -6, & 7, & -13, & -9, & -4, & -5,\\ 1, & 7, & -9, & -5, & -6, & -13, & -4, & 1, & 7, & -9, & -5, & -6, & -13, & -4,\end{matrix}
\end{aligned}$$

IX.	1,	-7,	-9,	5,	-6,	13,	-4,	-1,	7,	9,	-5,	6,	-13,	4,
X.	1,	9,	-6,	4,	7,	5,	-13,	-1,	-9,	6,	-4,	-7,	-5,	13,
X.	1,	-9,	-6,	-4,	7,	-5,	-13,	1,	-9,	-6,	-4,	7,	-5,	-13,
XI.	1,	13,	-5,	-7,	-4,	6,	-9,	-1,	-13,	5,	7,	4,	-6,	9,
XIII.	1,	-13,	-5,	7,	-4,	-6,	-9,	1,	-13,	-5,	7,	-4,	-6,	-9.

40. Hence before we conclude anything, we will set out the case also, where q is the product from two other prime numbers. Therefore the divisor shall be $p = 31$ and $q = 15 = 3 \cdot 5$, in which case the remainders are

$$1,\ 4,\ 9,\ -15,\ -6,\ 5,\ -13,\ 2,\ -12,\ 7,\ 3,\ 11,\ 14,\ 10,\ 8,$$

from which the following geometric progressions are formed, where indeed I add to each below,

I.	1,	4	-15,	2,	8,	1	4,	-15,	2,	8,	1,	4,	-15,	2	8,
II.	1,	8,	2,	-15,	4,	1,	8,	2,	-15,	4,	1,	8,	2,	-15	4,
III.	1,	9,	-12,	-15,	-11,	-6,	8,	10,	-3,	4	5,	14,	2,	-13,	7,
IV.	1,	7,	-13,	2,	14,	5,	4,	-3,	10,	8,	-6,	-11,	-15,	-12,	9,
V.	1,	2,	4,	8,	-15,	1,	2,	4,	8,	-15,	1,	2,	4,	8,	-15,
VI.	1,	-15,	8,	4,	2,	1,	-15,	8,	4,	2,	1,	-15,	8,	4,	2,
VII.	1,	-3,	9,	4,	-12,	5,	-15,	14,	-11,	2,	-6,	-13,	8,	7,	10,
VIII.	1,	10,	7,	8,	-13,	-6,	2,	-11,	14,	-15,	5,	-12,	4,	9,	-3,
IX.	1,	5,	-6,	1,	5,	-6,	1,	5,	-6,	1,	-5,	-6,	1,	5,	-6,
X.	1,	-6,	5,	1,	-6,	5,	1,	-6,	5,	1,	-6,	5,	1,	-6,	5,
XI.	1,	-11,	-3,	2,	9,	-6,	4,	-13,	-12,	8,	5,	7,	-15,	10,	14,
XII.	1,	14,	10,	-15,	7,	5,	8,	-12,	-13,	4,	-6,	9,	2,	-3,	-11,
XIII.	1,	-12,	-11,	8,	-3,	5,	2,	7,	9,	-15,	-6,	10,	4,	14,	-13,
XIV.	1,	-13,	-14,	4,	10,	-6,	-15,	9,	7,	2,	5,	-3,	8,	-11,	-12.

41. It is soon apparent by looking at these progressions some to be complete, of which the terms may show all the remainders, truly others to be periodic, which clearly depend on two or more periods, in which the same remainders recur in the same order, as it will help to note properly the distinction between complete and period progressions. Evidently periodic progressions are found, when with the prime divisor put in place $p = 2q + 1$ the number q can be resolved into two factors, so that there shall be $q = mn$; for moreover geometric progressions of this kind will be given, which contain m periods including some n remainders; and indeed just as many will be able to be assigned, as the number of ones contained in $n - 1$. For since all the powers of each term occur in the same period, it is evident a similar progression to be produced for each denominator taken, unless

perhaps the number of the periods thus may be doubled or multiplied, that is, it may be subdivided into two or more periods.

42. But from the complete expression, whatever that shall be, all the remaining are formed easily, whether they may be complete or periodic. Indeed the prime divisor shall be $p = 2q+1$ and this shall become a complete progression :

$$\begin{aligned} &\text{indices} \quad 0,\ 1,\ \ 2,\ \ 3,\ \ 4,\ \ 5,\cdots\cdots q-1,\\ &\text{progression } 1,\ \alpha,\ \alpha^2,\alpha^3,a^4,\ a^5,\cdots\cdots \alpha^{q-1}; \end{aligned}$$

hence if the terms may be picked out in equal jumps

$$\begin{aligned} &0,\ \ n,\ \ \ 2n,\ \ 3n,\ \ 4n,\cdots nq-n,\\ &1,\ \alpha^n,\ \alpha^{2n},\alpha^{3n},\ \alpha^{4n},\ \cdots\alpha^{nq-n}, \end{aligned}$$

this progression will be complete, if the number *n* were prime to *q* ; but if *n* and *q* may have a common divisor, for example *d,* then this progression will have just as many periods, with the number $\frac{q}{d}$ of which recurring in the same remainders, but the rest thence will be excluded completely. Moreover the number of these periods will define the common divisor between *n* and *q*. But truly in turn the complete progression will not be able to be formed from a periodic progression.

43. But in the first place this deserves to be noted in all these progressions : the sum of all the terms always to be equal to nothing, or to be divisible by the divisor *p* , which may be demonstrated in this manner. Since $a^q - 1$ may be granted to be divisible by *p*, but this form may be resolved into the factors

$$\alpha - 1 \text{ and } 1+\alpha+\alpha^2+\alpha^3+\ \cdots+\alpha^{q-1},$$

of which that one $\alpha - 1$ certainly is not divisible by *p* , by necessity it is this other, that is the sum of all the powers of our progression, allowed to be divided by the number *p*. And if the progression may have a period, the terms of each period assumed joined or the sum of all the remainders thence arising will be divisible by *p*, that which is itself evident from the examples advanced in the above examples.

44. But it is gathered from the same source, if the geometric progression were complete and *q* may have a factor *m,* so that there shall be $q = mn$ and the prime divisor $p = 2mn+1$, then on account of the form, $\alpha^{mn} - 1$ is divisible by $\alpha^m - 1$, which does not prove to be divisible by p , because the progression in any case may not be complete, indeed the quotient thence arises :

$$1+\alpha^m+\alpha^{2m}+\alpha^{3m}+\ \cdots+\alpha^{(n-1)m},$$

to become divisible by the divisor p. On account of which if the whole progression may be distributed into m parts in this manner :

$$1,\ \alpha,\ \cdots\ \alpha^{m-1}\ \big|\ \alpha^{m},\ \alpha^{m+1},\cdots\ \alpha^{2m-1}\ \big|\ \alpha^{2m},\ \alpha^{2m+1},\cdots\ \alpha^{3m-1}\ \big|\ \cdots\ \alpha^{(n-1)m},\cdots\ \alpha^{mn-1},$$

of which the number of members is $n,$ and thus these parts may themselves be written backwards [for negative remainders]:

1	$\alpha,$	$\alpha^2,$	$\cdots\alpha^{m-1},$
$\alpha^m,$	$\alpha^{m+1},$	$\alpha^{m+2},$	$\cdots\ \alpha^{2m-1},$
α^{2m}	$\alpha^{2m+1},$	$\alpha^{2m+2},$	$\cdots\ \alpha^{3m-1},$
..	..	..	..
..	..	..	..
$\alpha^{(n-1)m}$	$\alpha^{(n-1)m+1}$	$\alpha^{(n-1)m+2}$	$\cdots\ \alpha^{nm-1},$

then the sums of the terms placed in any of the vertical columns will be reduced to zero, or they will be divisible by the prime divisor $p = 2mn+1$. Moreover a complete progression made from different kinds can be distributed into just as many parts of this kind, as the number of divisors q will have had.

45. But the first vertical column will give the periods for all the periodic progressions. From these numbers being understood not only these to be the remainders of squares, but also of the even powers of higher orders. Evidently if the prime divisor shall be of this form $p = 2mn+1$, just as only half of mn has occurred in the remainders of squares among the smaller number themselves, of which the number is $= 2mn,$ and the same number thence is excluded, thus on dividing the powers $2m$ of the exponent by the same number p only n different divisors thence result and all the rest, of which the number is $(2m-1)n$, having been prepared thus, so that in no way may they be contained in the form $a^{2m} - ip$, or no exponent of the power $2m$ shall be able to be shown, which becomes divisible by any of these numbers, decreased by the prime number $p = 2mn+1$.

46. And neither indeed has this property been restricted to the powers of even exponents, but it can be stated in general, if a prime divisor shall be of the form $p = mn+1$, which clearly diminished by one may be resolved into factors m and n , and the powers of the exponent $m,$ surely :

$$1,\ 2^m,\ 3^m,\ 4^m,\ 5^m,\ 6^m,\cdots(p-1)^m,$$

may be divided by that, then among the remainders only n different numbers occur, of which the individuals m may be repeated in turn, but all the remaining numbers, of which the number is $(m-1)n$, hence may be excluded ; from which significant properties of the

numbers which are the powers can be acknowledged in the account of the divisibility by prime number.

47. Therefore since there is no doubt, why hence many outstanding properties of numbers may not be elicited, the examples of several prime numbers has been seen to be added here, and from these the remainders, which arise from the division of the powers, show where certain reciprocal numbers may be represented together:

l. Divisor $p = 3 = 2+1$	2. Divisor $p = 5 = 2\cdot 2+1$
Powers Remainder	Powers Remainder
a^2 $\{1$	a^2 $\{1,-1$
	a^4 $\{1,$
3. Divisor $p = 7 = 2\cdot 3+1$	4. Divisor $p = 11 = 2\cdot 5+1$
Powers Remainder	Powers Remainder
a^2 $\begin{cases}1,\ 2\\ -3\end{cases}$	a^2 $\begin{cases}1,\ 4,\ 5,\\ 3,-2\end{cases}$
a^3 $\{1,\ -1$	a^5 $\{1,\ -1$
a^6 $\{1$	a^{10} $\{1$
5. Divisor $p = 13 = 2\cdot 2\cdot 3+1$	6. Divisor $p = 17 = 2^4+1$
Powers Remainder	Powers Remainder
a^2 $\begin{cases}1,\ 4,\ 3,-1\\ -3,-4\end{cases}$	a^2 $\begin{cases}1,\ 2,\ 4,\ 8,-1\\ -8,-4,\ -2\end{cases}$
a^3 $\begin{cases}1,\ -5,-1\\ 5\end{cases}$	a^4 $\begin{cases}1,\ 4,-1\\ -4\end{cases}$
a^4 $\begin{cases}1,\ 3\\ -4\end{cases}$	a^8 $\{1,\ -1$
a^6 $\{1,\ -1$	a^{16} $\{1$
a^{12} $\{1$	

7. Divisor $p = 19 = 2\cdot 3\cdot 3+1$

Powers	Remainder
a^2	$\begin{cases} 1, & 4, & -3, & 7, & 9 \\ & 5, & 6, & -8, & -2 \end{cases}$
a^3	$\begin{cases} 1, & 8, & 7, & -1 \\ & -7, & -8 \end{cases}$
a^6	$\begin{cases} 1, & 7 \\ & -8 \end{cases}$
a^9	$\{1, \ -1$

8. Divisor $p = 23 = 2\cdot 11+1$

Powers	Remainder
a^2	$\begin{cases} 1, 4, & -7, & -5, 3, & -11 \\ & 6, & -10, & 9, 8, & 2 \end{cases}$
a^{11}	$\{1, \ -1$

9. Divisor $p = 29 = 2\cdot 2\cdot 7+1$

Powers	Remainder
a^2	$\begin{cases} 1, & 4, -13, & 6, -5, & 9, & 7, -1 \\ & -7, -9, & 5, -6, & 13, -4 \end{cases}$
a^4	$\begin{cases} 1, -13, & -5, & 7 \\ & -9, & -6, & -4 \end{cases}$
a^7	$\begin{cases} 1, & 12, & -1 \\ & -12 \end{cases}$
a^{14}	$\{1, \ -1$

10. Divisor $p = 31 = 2\cdot 3\cdot 5+1$

Powers	Remainder
a^2	$\begin{cases} 1, & 9, -12, & -15, -11, & -6, & 8, & 10 \\ & 7, -13, & 2, & 14, & 5, & 4, & -3 \end{cases}$
a^3	$\begin{cases} 1, & -4, -15, & -2, & 8, & -1 \\ & -8, & 2, & 15, & 4 \end{cases}$
a^5	$\begin{cases} 1, & -5, & -6, & -1 \\ & 6, & 5 \end{cases}$
a^6	$\begin{cases} 1, & 2, & 4 \\ & -15, & 8 \end{cases}$
a^{10}	$\begin{cases} 1, & 5 \\ & -6 \end{cases}$
a^{15}	$\{1, \ -1$

11. Divisor $p = 37 = 2 \cdot 2 \cdot 3 \cdot 5 + 1$

Powers	Remainder
a^2	$\left\{\begin{array}{l} 1,\ 4,\ 16,\ -10,\ -3,\ -12,\ -11,\ -7,\ 9,\ -1 \\ -9,\ 7,\ 11,\ 12,\ 3,\ 10,\ -16,\ -4 \end{array}\right.$
a^3	$\left\{\begin{array}{l} 1,\ 8,\ -10,\ -6,\ -11,\ -14,\ -1 \\ 14,\ 11,\ 6,\ 10,\ -8 \end{array}\right.$
a^4	$\left\{\begin{array}{l} 1,\ 16,\ -3,\ -11,\ 9 \\ 7,\ 12,\ 10,\ -4 \end{array}\right.$
a^6	$\left\{\begin{array}{l} 1,\ -10,\ -11,\ -1 \\ 11,\ 10 \end{array}\right.$
a^9	$\left\{\begin{array}{l} 1,\ -6,\ -1 \\ 6 \end{array}\right.$
a^{12}	$\left\{\begin{array}{l} 1,\ -11 \\ 10 \end{array}\right.$
a^{18}	$\{1,\ -1$

12. Divisor $p = 41 = 2^3 \cdot 5 + 1$

Powers	Remainder
a^2	$\left\{\begin{array}{l} 1,\ -2,\ 4,\ -8,\ 16,\ 9,\ -18,\ -5,\ 10,\ -20,\ -1 \\ 20,\ -10,\ 5,\ 18,\ -9,\ -16,\ 8,\ -4\ \ 2 \end{array}\right.$
a^4	$\left\{\begin{array}{l} 1,\ 4,\ 16,\ -18,\ 10,\ -1 \\ -10,\ 18,\ -16,\ -4 \end{array}\right.$
a^5	$\left\{\begin{array}{l} 1,\ -3,\ 9,\ 14,\ -1 \\ -14,\ -9,\ 3 \end{array}\right.$
a^8	$\left\{\begin{array}{l} 1,\ 16,\ 10 \\ 18,\ -4 \end{array}\right.$
a^{10}	$\left\{\begin{array}{l} 1,\ 9,\ -1 \\ -9 \end{array}\right.$
a^{20}	$\{1,\ -1$

13. Divisor $p = 43 = 2 \cdot 3 \cdot 7 + 1$

Powers	Remainder
a^2	$\begin{cases} 1, & 9, & -5, & -2, & -18, & 10, & 4, & -7, & -20, & -8, & 14 \\ -19, & 17, & 21, & -12, & 13, & 11, & 6, & 15, & 16, & -3 \end{cases}$
a^3	$\begin{cases} 1, & 8, & 21, & -4, & 11, & 2, & 16, & -1 \\ -16, & -2, & -11, & 4, & -21, & -8 \end{cases}$
a^6	$\begin{cases} 1, & 21, & 11, & 16 \\ -2, & 4, & -8 \end{cases}$
a^7	$\begin{cases} 1, & 6, & -7, & -1 \\ 7, & 6 \end{cases}$
a^{14}	$\begin{cases} 1, & -7 \\ 6 \end{cases}$
a^{21}	$\{1, \quad -1$

14. Divisor $p = 47 = 2 \cdot 23 + 1$

Powers	Remainder
a^2	$\begin{cases} 1, & 4, & 16, & 17, & 21, & -10, & 7, & -19, & 18, & -22, & 6, & -23 \\ 12, & 3, & -11, & 9, & 14, & -20, & -5, & -13, & -15, & 8, & 2 \end{cases}$
a^{23}	$\{1, \ -1$

15. Divisor $p = 53 = 2 \cdot 2 \cdot 13 + 1$

Powers	Remainder
a^2	$\begin{cases} 1, & 4, & 16, & 11, & -9, & 17, & 15, & -7, & -25, & 6, & 24, & -10, & 13, & -1 \\ -13, & 10, & -24, & -6, & 25, & -7, & -15, & -17, & 9, & -11, & -16, & -4 \end{cases}$
a^4	$\begin{cases} 1, & 16, & -9, & 15, & -25, & 24, & 13 \\ 10, & -6, & -7, & -17, & -11, & -4 \end{cases}$
a^{13}	$\begin{cases} 1 & -23, & -1 \\ 23 \end{cases}$
a^{26}	$\{1, \ -1$

16. Divisor $p = 59 = 2 \cdot 29 + 1$

Powers	Remainder
a^2	$\begin{cases} 1, & 4, & 16, & 5, & 20, & 21, & 25, & -18, & -13, & 7, & 28, & -6, & -24, & 2 \\ 15, & -11, & 12, & 3, & -14, & 26, & -23, & 9, & 17, & 19, & -10, & 27, & -8 \end{cases}$
a^{29}	$\{1, \ -1$

17. Divisor $p = 61 = 2 \cdot 2 \cdot 3 \cdot 5 + 1$

Powers	Remainder
a^2	$\begin{cases} 1, & 4, & 16, & 3, & 12, & -13, & 9, & -25, & 22, & 27, & -14, & 5, & 20, & 19, & 15, \\ -15, & -19, & -20, & -5, & 14, & -27, & -22, & 25, & -9, & 13, & -12, & -3, & -16, & -4 \end{cases}$
a^3	$\begin{cases} 1, & 8, & 3, & 24, & 9, & 11, & 27, & -28, & 20, & -23, & -1 \\ 23, & -20, & 28, & -27, & -11, & -9, & -24, & -3, & -8 \end{cases}$
a^4	$\begin{cases} 1, & 16, & 12, & 9, & 22, & -14, & 20, & 15 \\ -19, & -5, & -27, & 25, & 13, & -3, & -4 \end{cases}$
a^5	$\begin{cases} 1, & -29, & -13, & 11, & -14, & -21, & 15 \\ 21, & 14, & -11, & 13, & 29, & -1 \end{cases}$
a^6	$\begin{cases} 1, & 3, & 9, & 27, & 20, & -1 \\ -20, & -27, & -9, & -3 \end{cases}$
a^{10}	$\begin{cases} 1, & -13, & -14, & -1 \\ 14, & 13 \end{cases}$
a^{12}	$\begin{cases} 1, & -3, & 9, & -1 \\ 20, & -27 \end{cases}$
a^{15}	$\begin{cases} 1, & 11, & -1 \\ -11, \end{cases}$
a^{20}	$\begin{cases} 1, -14 \\ 13, \end{cases}$
a^{30}	$\{1, -1$

CONCLUSION

CONCERNING THE POWERS OF EACH ORDER AND WITH THE REMAINDERS LEFT IN THE DIVISION OF THESE BY PRIME NUMBERS

48. Just as in these examples the remainders have been shown for the individual powers by geometric progressions, which likewise continued backwards represent the associated remainders linked together, thus likewise for powers of the first order it can arise, where indeed plainly all the numbers with smaller divisors must occur, thus so that, if the prime divisor shall be $p = 2q + 1$, the number of different remainders shall be $= 2q$, which will be reduced to the smallest form $\pm 1,\ \pm 2,\ \pm 3,\ \pm 4$ etc. as far as to $\pm q$. Truly all these remainders can be set out too following geometric progressions beginning from unity, provided that its denominator or the number following the second term may be accepted, which all plainly may produce numbers which arise if this there prepared thus, so that no power of that, of which the exponent shall be less than $2q$, may leave one for the

remainder. But it is certain such numbers given for any divisor, even if these may be seen to be assigned with the greatest difficulty and the natures of these being referred to the deepest mysteries of numbers.

49. Therefore in general for the prime divisor $p = 2q+1$, the letter *a* shall be a number of this kind, whose powers divided by *p* leave for remainders all the numbers less than p itself, nor before one recurs in the geometric series

$$1,\ a,\ a^2,\ a^3,\ a^4 \text{ etc.}$$

shall it have arrived at the power a^{2q}, certainly which divided by $p = 2q+1$ always leaves the remainder one, and thus all the powers may be produced here with different remainders. Therefore since the power a^q cannot leave one as the remainder and since $a^{2q}-1 = (a^q+1)(a^q-1)$, a^q+1 will be divisible by *p* and the power a^q will give the remainder -1; then truly the following powers a^{q+1}, a^{q+2}, a^{q+3}, etc. will give the remainders $-a, -a^2, -a^3$ etc., which thus have been prepared, so that with the antecedents a^{q-1}, a^{q-2}, a^{q-3}, etc., they may show the two remainders associated together, clearly the product of which a^{2q} may be equivalent to unity. Therefore we will be able to represent these remainders in the following manner by the association :

Indices	0,	1,	2 ,	3,	4,	$q-3$,	$q-2$,	$q-1$,	q
	1,	a^1,	a^2,	a^3,	a^4, ….	a^{q-3},	a^{q-2},	a^{q-1},	-1,
		$-a^{q-1}$,	$-a^{q-2}$,	$-a^{q-3}$,	$-a^{q-4}$, ...	$-a^3$,	$-a^2$,	$-a$	
indices	$2q$,	$2q-1$,	$2q-2$,	$2q-3$,	$2q-4$,	$q+3$,	$q+2$,	$q+1$,	q

where the two remainders themselves have been written below between the associated remainders themselves, truly with the ends $+1$ and -1 alone, certainly which are themselves associated with that number.

50. From such a geometric progression put in place, which all the remainders arising from powers of the first order, that is clearly it embraces all the numbers, from that all the remainders may become known for the powers of any order, clearly by retaining the same prime divisor $p = 2q+1$.

Without doubt the remainders arising from the division of the squares will be

$$1,\ a^2,\ a^4,\ a^6,\ a^8\ \ldots\ a^{2q-2},$$

which correspond to even indices only, and may be shown thus by association :

$$\begin{array}{lllll} & a^2, & a^4, & a^6, & a^8 \quad \text{etc.} \\ 1, & & & & \\ & -a^{q-2}, & -a^{q-4}, & -a^{q-6}, & -a^{q-8} \quad \text{etc.} \end{array}$$

in which therefore -1 will be found, if q were an even number.

But for the cubes only these terms can be accepted, of which the indices are multiples of three,

$$1,\ a^3,\ a^6,\ a^9 \text{ etc.}$$

From which it is apparent, if the exponent $2q$ may admit division by 3, the number of remainders to be rendered by multiples of three, while in the remaining cases clearly all the remainders occur.

In a similar manner the remainders of the fourth power may be obtained from the indices divisible by 4, or from these powers

$$1,\ a^4,\ a^8,\ a^{12} \text{ etc.}$$

and the remainders of the fifth powers from these

$$1,\ a^5,\ a^{10},\ a^{15} \text{ etc.}$$

51. Therefore there is still a need, in order that for any prime divisor $p = 2q+1$, suitable numbers may be had for a, from the powers of which clearly all the remainders may emerge; but for which I am forced to admit nevertheless, no certain rule to be known to me. At any rate it will help for this to be noted, if one number of this kind a were known, its associate [*i.e.* reciprocal or inverse], which shall be b, so that $ab-1$ may become divisible by p, also to be of the appropriate aforesaid parity; moreover we can see this can be shown of the associate b either by a^{2q-1} or by $-a^{q-1}$. From which it is allowed to conclude also that for a, any of its powers a^n can be taken, of which the exponent n shall be prime to the number $2q$, where indeed it suffices with the number n for $2q$ to be assumed smaller, since the same remainders may be repeated from the higher powers. Truly now since a certain law lies hidden, I will show for the more simple divisors on assuming suitable numbers for a, evidently from the powers of which clearly all the remainders may arise [*note*: the actual remainders are not shown in this table] :

Prime divisors	Numbers required to be assumed for a
$p=3\,,q=1$	-1
$p=5,q=2$	± 2
$p=7,q=3$	$-2,\ +3$
$p=11,\ q=5$	$+2,-3,\ -4,-5$
$p=13,\ q=6$	$\pm 2,\ \pm 6$
$p=17,\ q=8$	$\pm 3,\ \pm 5,\ \pm 6,\ \pm 7$
$p=19,q=9$	$+2,+3,\ -4,\ -5,\ -6,\ -9$
$p=23,\ q=11$	$-2,\ -3,\ -4,\ +5,\ -6,\ +7,\ -8,\ -9,\ +10,\ +11$
$p=29,\ q=14$	$\pm 2,\ \pm 3,\ \pm 8,\ \pm 10,\ \pm 11,\ \pm 14$
$p=31,\ q=15$	$+3,\ -7,\ -9,\ -10,\ +11,\ +12,\ +13,\ -14$
$p=37,q=18$	$\pm 2,\ \pm 5,\ \pm 13,\ \pm 15,\ \pm 17,\ \pm 18$
$p=41,q=20$	$\pm 6,\ \pm 7,\ \pm 11,\ \pm 12,\ \pm 13,\ \pm 15,\ \pm 17,\ \pm 19$

52. In the latter case $p=41$ therefore it appears not possible for a number less than 6 to be assumed for a , since in the preceding geometric progressions it may be able to be formed from smaller numbers; from which for this divisor $p=41$ this same progression thus will itself be had [e.g. $6^2=36=(41\times 0)-5$; $6^3=216=(41\times 5)+11$; etc.]:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1,	$+6,-5,+11,-16,-14,-2,-12,+10,+19,-9,-13,+4,-17,-20,+3,+18,-15,-8,-7$																			-1
	$+7,+8,+15,-18,-3,+20,+17,-4,+13,+9,-19,-10,+12,+2,+14,+16,-11,+5,-6$																			

Hence if these numbers may be removed, which correspond to even indices, the remainders will be had arising from the squares; but if these may be removed, which agree with the indices either for the divisors 4, 5, 8, 10, or 20, the remainders for the same named powers will be obtained, and these same ones, which now have been examined above [in § 47]. And the account is similar for all the remaining prime numbers.

53. However, so that a may extend to all of these numbers, I observe that in any case $p=2q+1$ to be equal to the sum of these numbers smaller than p, which shall be prime to $2q$; and I have shown elsewhere for this sum requiring to be found, the number $2q$ must be resolved into its prime factors, thus so that, if there were

$$2q=f^{\zeta}g^{\eta}h^{\theta}k^{\chi},$$

this

$$=(f-1)^{\zeta}(g-1)^{\eta}(h-1)^{\theta}(k-1)^{\chi}.$$

But for any number defined $p = 2q + 1$ for this amount shall be the numbers prime to $2q$ 1, α, β, γ, δ etc., and if any one number a were given, thus all the remaining will be

$$a,\ a^{\alpha} - np,\ a^{\beta} - np,\ a^{\gamma} - np,\ a^{\delta} - np,\ \text{etc.}$$

by taking n thus, so that all these number less than p may be removed. Perhaps this consideration will find a way for any case requiring these numbers to be investigated.

DISQUISITIO ACCURATIOR CIRCA RESIDUA EX DIVISIONE QUADRATORUM ALTIORUMQUE POTESTATUM PER NUMEROS PRIMOS RELICTA

Opuscula analytica 1, 1783, p. 121-156

1. Si numerus quadratus *aa* per numerum primum *p* dividatur, residuum relictum littera α indicetur; similique modo litterae β, γ, δ etc. mihi denotabunt residua in divisione quadratorum *bb, cc, dd* etc. relicta.

2. Erit ergo $\alpha = aa - np$, quia residuum α prodit, si a quadrato *aa* multiplum numeri *p* auferatur idque maximum, ut residuum α ipso divisore *p* minus reddatur. Nihil autem impedit, quominus multiplum *np* maius accipiatur quadrato *aa,* unde residuum α prodit negativum, sicque eius valor infra $\frac{1}{2}p$ deprimi potest.

3. Idem igitur residuum *a* multis modis exhiberi potest, quoniam cunctae hae formae $\alpha \pm mp$ eandem naturam continent. Perinde scilicet est, sive residuum ex divisione quadrati *aa* per numerum *p* ortum dicatur esse α sive $\alpha \pm p$ sive $\alpha \pm mp$ denotante littera *m* numerum integrum quemcumque.

4. Innumera autem quadrata *aa* per numerum *p* divisa idem relinquunt residuum α, quae omnia ex cognito uno *aa* facile inveniuntur. Cuncta haec quadrata ista forma $(a \pm mp)^2$ vel $(mp \pm a)^2$ contineri evidens est sicque sufficit residuum ex harum forma minima, cuius radix non excedet $\frac{1}{2}p$, notasse; omnia scilicet haec quadrata $(mp \pm a)^2$ respectu numeri *p* eiusdem indolis sunt censenda.

5. Quadratis secundum ordinem naturalem dispositis residua per divisorem *p* orta ita se habebunt:

Quadrata	$1^2, 2^2, 3^2, 4^2,$	$\cdots\cdots$	$(p-4)^2, (p-3)^2, (p-2)^2, (p-1)^2,$								
Residua	1,	4,	9,	16,	$\cdots\cdots$	16,	9,	4,	1.		

Quadratis ergo ad $(p-1)^2$ continuatis singula residua his occurrunt; et quia *p* est numerus primus, eorum numerus est par et bina quadrata media $\left(\frac{p-1}{2}\right)^2$ et $\left(\frac{p+1}{2}\right)^2$ idem dabunt residuum $\frac{pp-2p+1}{4}$.

6. Omnia ergo residua, quae quidem ex divisione numerorum quadratorum per numerum primum p resultare possunt, nascuntur ex his quadratis:

$$\text{Quadrata} \quad 1^2, 2^2, 3^2, 4^2, \quad \ldots\ldots \quad \left(\tfrac{p-1}{2}\right)^2,$$
$$\text{Residua} \quad 1, \quad 4, \quad 9, \quad 16, \quad \ldots\ldots \quad \tfrac{pp-2p+1}{4}.$$

quorum numerus est $= \frac{p-1}{2}$. Neque ergo omnes numeri divisore p minores, quorum multitudo est $p-1$, inter residua occurrunt, sed eorum semissis inde certe excluditur.

7. Continuatis autem quadratis ad $\left(\frac{p-1}{2}\right)^2$ residua inde orta omnia sunt diversa; neque enim ullum usque ad hunc terminum bis occurrere potest, siquidem divisor p sit numerus primus. Namque si bina quadrata aa et bb neutro quadratum $\left(\frac{p-1}{2}\right)^2$ excedente idem darent residuum r, differentia eorum $aa-bb$ ideoque vel $a-b$ vel $a+b$ per p dividi posset. Cum autem neque a neque b superet $\frac{p-1}{2}$, etiam summa $a+b$ minor erit quam p ideoque fieri omnino nequit, ut ea summa ac multo minus differentia $a-b$ divisionem per numerum p admittat.

8. Proposito ergo numero primo p omnia residua ex his quadratis

$$1^2, 2^2, 3^2, 4^2, \quad \ldots\ldots \quad \left(\tfrac{p-1}{2}\right)^2$$

obtinentur; quorum numerus cum sit $= \frac{p-1}{2}$ et residua omnia inter se differant, numerorum ipso p minorum, quorum multitudo est $p-1$, semissis certe inter residua occurrit; semissis vero inde excluditur et classem *non-residuorum* constituit. Pro quolibet ergo numero primo p residua a nonresiduis probe sunt discernenda.

9. Si enim α inter residua occurrat, pronunciare possumus innumerabilia quadrata dari, quae in hac forma $np+\alpha$ contineantur, ac minimi eorum radicem non excedere numerum $\frac{p-1}{2}$. Sin autem numerus $\mathfrak{A}$ inter residua non reperiatur, pronunciabimus nullum numerum quadratum in forma $np+\mathfrak{A}$ contineri. Quovis autem casu tam residuorum α quam non-residuorum $\mathfrak{A}$ multitudo est $= \frac{p-1}{2}$.

10. Quodsi residua ex divisione quadratorum per numerum primum p oriunda secundum hunc ordinem naturalem disponantur, primo occurrent numeri quadrati 1, 4, 9, 16 etc., donec divisione per numerum p ad minores numeros redigi possunt; postremum vero eorum erit $\frac{pp-2p+1}{4}$, unde numerum p, quoties fieri potest, auferri oportet.

11. Ad hoc postremum residuum agnoscendum duos casus contemplari convenit, prout numerus primus p fuerit formae vel $4q+1$ vel $4q+3$.

Sit primo $p=4q+1$ ideoque $\frac{p-1}{2}=2q$ et ultimum residuum $4qq$, quod subtractione multipli $qp=4qq+q$ reducitur ad $-q$ seu ad $3q+1$.

Altero vero casu $p=4q+3$ seu $\frac{p-1}{2}=2q+1$ ultimum residuum $4qq+4q+1$ ablatione multipli $qp=4qq+3q$ reducitur ad $q+1$.

12. Simili modo penultimum residuum ex quadrato $\left(\frac{p-3}{2}\right)^2$ ortum reperitur

pro casu $p=4q+1: 4qq-4q+1$ seu $-5q+1$ seu $-q+2$,
pro casu $p=4q+3: 4qq$ seu $-3q$ seu $q+3$.

At antepenultimum ex $\left(\frac{p-5}{2}\right)^2$ ortum ita prodit

pro casu $p=4q+1: 4qq-8q+4$ seu $-9q+4$ seu $-q+6$,
pro casu $p=4q+3: 4qq-4q+1$ seu $-7q+1$ seu $q+7$.

Quod vero antepenultimum praecedit, hoc modo

pro casu $p=4q+1: 4qq-12q+9$ seu $-13q+9$ seu $-q+12$,
pro casu $p=4q+3: 4qq-8q+4$ seu $-11q+4$ seu $q+13$.

13. Hos igitur binos casus distinguendo residua sequenti modo se habebunt;

Casu $p=4q+1$:

Quadrata $1,\ 2^2,\ 3^2,\ 4^2,\ \cdots\ (2q-3)^2,\ (2q-2)^2,\ (2q-1)^2,\ (2q)^2,$
Residua $1,\ 4,\ 9,\ 16,\ \cdots\ -q+12,\ -q+6,\ -q+2,\ -q$
seu $3q+13,\ 3q+7,\ 3q+3,\ 3q+1.$

Casu $p=4q+3$:

Quadrata $1,\ 2^2,\ 3^2,\ 4^2,\ \cdots\ (2q-2)^2,\ (2q-1)^2,\ (2q)^2,\ (2q+1)^2,$
Residua $1,\ 4,\ 9,\ 16,\ \cdots\ q+13,\ q+7,\ q+3,\ q+1.$

Priori scilicet casu in genere occurrit residuum $-q+nn+n$ seu $3q+nn+n+1$,
posteriori vero $q+nn+n+1$.

14. Quo hic residuorum ordo clarius perspiciatur, exempla spectanda proponam et primo quidem pro numeris primis formae $p=4q+1$.

$p=5\begin{cases}1,\ 2^2,\\ q=1\\ 1,\ 4\end{cases}$

seu $1,-1$

$p=13\begin{cases}1,\ 2^2\ ,3^2\ ,4^2\ ,5^2\ ,6^2\\ q=\ 3\\ 1,\ 4,\ \ 9,\ \ 3,\ 12,\ 10\end{cases}$

seu $1,\ 4,-4,\ \ 3,-1,\ -3$

$p=17\begin{cases}1,\ 2^2\ ,3^2\ ,4^2\ ,5^2\ ,6^2,7^2\ ,8^2\\ q=\ 4\\ 1,\ 4,\ \ 9,\ 16,\ \ 8,\ \ 2,\ 15,\ 13\end{cases}$

seu $1,\ 4,-8,\ -1,\ \ 8,\ \ 2,\ -2,-4$

$p=29\begin{cases}1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ \ 8^2,\ 9^2,\ 10^2,\ 11^2,\ 12^2,\ 13^2,\ 14^2\\ q=\ 7\\ 1,\ 4,\ \ 9,\ 16,\ \ 25,\ 7,\ 20,\ \ 6,\ \ 23,\ 13,\ \ 5,\ \ 28,\ \ 24,\ \ 22\end{cases}$

seu $1,\ 4,\ \ 9,-13,\ -4,\ 7,-9,\ \ 6,\ -6,\ 13,\ \ 5,\ \ -1,\ \ -5,\ \ -7$

$p=37\begin{cases}1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ \ 8^2,\ 9^2,\ 10^2,\ 11^2,\ 12^2,\ 13^2,\ 14^2,\ 15^2,\ 16^2,\ 17^2,\ 18^2\\ q=\ 9\\ 1,\ 4,\ \ 9,\ 16,\ \ 25,\ 36,\ 12,\ 27,\ 7,\ 26,\ \ 10,\ \ 33,\ \ 21,\ \ 11,\ \ \ 3,\ \ 34,\ \ \ 30,\ 28\end{cases}$

seu $1,\ 4,\ \ 9,\ 16,-12,-1,\ \ 12,-10,\ 7,-11,\ \ 10,\ \ -4,-16,\ \ 11,\ \ \ 3,\ \ -3,\ \ -7,\ \ -9$

$p=41\begin{cases}1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ \ 8^2,\ 9^2,\ 10^2,\ 11^2,\ 12^2,\ 13^2,\ 14^2,\ 15^2,\ 16^2,\ 17^2,\ 18^2,\ 19^2,\ 20^2\\ q=\ 10\\ 1,\ 4,\ \ 9,\ 16,\ \ 25,\ 36,\ 8,\ 23,\ 40,\ 18,\ \ 39,\ \ 21,\ \ \ 5,\ \ 32,\ \ \ 20,\ \ 10,\ \ \ 2,\ \ \ 37,\ \ \ 33,\ \ 31\end{cases}$

seu $1,\ 4,\ \ 9,\ 16,-16,-5,\ \ 8,-18,\ -1,\ \ 18,\ \ -2,-20,\ \ \ 5,\ -9,\ \ \ 20,\ 10,\ \ \ 2,\ -4,\ \ -8,-10$

Ubi observare licet in residuis per negativa ad minimam formam reductis singulos numeros bis, positive scilicet et negative, occurrere.

15. Sequentia exempla pertinent ad numeros primos formae $p=4q+3$.

$p=3\left\{\begin{matrix}1\\1\end{matrix}\right.$
$q=0$

$p=7\left\{\begin{matrix}1,\ 2^2,\ 3^2\\1,\ 4,\ \ 2,\end{matrix}\right.$
$q=1$
seu $\quad 1,-3,\ 2$

$p=11\left\{\begin{matrix}1,\ 2^2,\ 3^2,\ 4^2,\ 5^2\\1,\ 4,\ \ 9,\ \ 5,\ \ 3\end{matrix}\right.$
$q=\ 2$
seu $\quad 1,\ 4,-2,\ \ 5,\ \ 3$

$p=19\left\{\begin{matrix}1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ 8^2,\ 9^2\\1,\ 4,\ \ 9,\ 16,\ \ 6,\ \ 17,\ 11,\ 7,\ \ 5\end{matrix}\right.$
$q=\ 4$
seu $\quad 1,\ 4,\ \ 9,\ -3,\ \ 6,\ -2,\ -8,\ 7,\ \ 5$

$p=23\left\{\begin{matrix}1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ \ 8^2,\ 9^2,\ 10^2,\ 11^2\\1,\ 4,\ \ 9,\ 16,\ \ 2,\ \ 13,\ \ \ 3,\ \ 18,\ 12,\ 8,\ \ \ 6\end{matrix}\right.$
$q=\ 7$
seu $\quad 1,\ 4,\ \ 9,\ -7,\ \ 2,-10,\ \ \ 3,\ -5,-11,\ 8,\ \ \ 6$

$p=31\left\{\begin{matrix}1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ \ 8^2,\ 9^2,\ 10^2,\ 11^2,\ 12^2,\ 13^2,\ 14^2,\ 15^2\\1,\ 4,\ \ 9,\ 16,\ \ 25,\ \ 5,\ \ 18,\ \ 2,\ \ \ 19,\ \ 7,\ \ 20,\ \ 33,\ \ 14,\ \ \ 10,\ \ \ 8,\end{matrix}\right.$
$q=\ 5$
seu $\quad 1,\ 4,\ \ 9,-15,\ \ -6,\ \ 5,-13,\ \ 2,\ -12,\ \ 7,\ -11,-16,\ \ \ 14,\ \ \ 10,\ \ \ 8,$

$p=43\left\{\begin{matrix}1,\ 2^2,\ 3^2,\ \ 4^2,\ 5^2,\ 6^2,\ 7^2,\ \ 8^2,\ 9^2,\ 10^2,\ 11^2,\ 12^2,\ 13^2,\ 14^2,\ 15^2,\ 16^2,\ 17^2,\ 18^2,\ 19^2,\ \ 20^2,\ \ 21^2\\1,\ 4,\ \ 9,\ \ 16,\ \ 25,\ \ 36,\ \ 6,\ \ 21,\ \ 38,\ \ 14,\ \ \ 35,\ \ \ 15,\ \ \ 40,\ \ \ \ 4,\ \ 10,\ \ 41,\ \ \ 31,\ \ \ \ 23,\ \ 17,\ \ \ 13,\ \ \ 11\end{matrix}\right.$
$q=\ 10$
seu $\quad 1,\ 4,\ \ 9,\ \ 16,-18,-7,\ \ \ 6,\ \ 21,\ -5,\ \ 14,\ \ -8,\ \ \ 15,\ \ -3,\ \ -19,\ 10,\ \ -2,-12,\ \ -20,\ \ 17,\ \ \ 13,\ \ \ 11$

In istis residuis ad minimam formam reductis omnes plane numeri ab unitate usque ad $2q+1$ occurrunt, alii signo positionis, alii negationis affecti. Verum has proprietates observatas demonstrari oportet.

16. Iam supra, [*Observationes circa*…E552, Theorema II], demonstravi, si inter residua ex divisione quadratorum per numerum *p* orta occurrant numeri α et β, ibidem quoque reperiri productum $\alpha\beta$ ac proinde quoque hanc formam latius patentem $\alpha^m\beta^n$. Oriantur enim haec residua ex quadratis *aa* et *bb,* ita ut sit

$$aa=mp+\alpha \text{ et } bb=np+\beta,$$

atque manifestum est ex horum quadratorum producto

$$aabb = mnpp + (m\beta + n\alpha) + \alpha\beta,$$

cuius forma est $Mp + \alpha\beta$, nasci residuum $\alpha\beta$; similique modo ex quadrato $a^{2m}b^{2n}$ provenire residuum $\alpha^m\beta^n$ seu $a^m\beta^n - Mp$, ut ad minimam formam reducatur. Quin etiam notari convenit hoc ipsum residuum $\alpha^m\beta^n$ nasci ex omnibus his quadratis $(a^m b^n \pm Np)^2$ seu $(Np \pm a^m b^n)^2$ ideoque ex quadrato, cuius latus $a^m b^n - Np$ seu $Np - a^m b^n$ minus erit quam $\frac{1}{2}p$.

17. Denotent litterae

$$a,\ b,\ c,\ d,\ldots l$$

omnes numeros divisoris p semisse $\frac{1}{2}p$ minores, quorum ergo multitudo est $= \frac{p-1}{2}$, sintque

$$\alpha,\ \beta,\ \gamma,\ \delta,\ldots\lambda$$

residua ex eorum quadratorum

$$a^2,\ b^2,\ c^2,\ d^2,\ldots l^2$$

per numerum p divisione relicta, quorum multitudo itidem est $= \frac{p-1}{2}$, ita ut ex omnibus numeris divisore p minoribus, quorum multitudo est $p-1$, totidem ex residuorum ordine excludantur, quos nomine *non-residuorum* complexos litteris

$$\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \ldots \mathfrak{L}$$

indicabo. Notatu ergo maxime dignum est in ordine residuorum $\alpha,\ \beta,\ \gamma,\ \delta,\ldots\lambda$, etiamsi eorum multitudo tantum est $= \frac{p-1}{2}$, tamen omnia eorundem producta ex binis pluribusque atque etiam singulorum potestates omnes occurrere, siquidem auferendo inde, quoties fieri potest, divisorem p ad minimam formam revocentur.

18. Quo magis haec illustrentur, animadverti oportet ratione cuiusque divisoris p omnes numeros in totidem species distribui; scilicet ratione divisoris 2 duae habentur species numerorum parium et imparium formulis $2x$ et $2x+1$ contentorum. Divisor autem 3 tres praebet numerorum species $3x,\ 3x+1$ et $3x+2$ et divisor 4 has quatuor $4x,\ 4x+1,\ 4x+2$ et $4x+3$, quae diversae species in numerorum doctrina sollicite distingui solent. Simili ergo modo ratione divisoris cuiusque p hae diversae numerorum species constituuntur

$$px,\ px+1, px+2, px+3,\ \ldots px+p-1,$$

quarum multitudo est *p.* Omissa ergo prima specie *px* multipla divisoris *p* continente reliquarum multitudo est $p-1$, ac si *p* fuerit numerus primus, has species in duas classes dividi convenit utraque $\frac{p-1}{2}$ species complectente

$$px+\alpha,\ px+\beta,\ px+\gamma,\ px+\delta,...px+\lambda,$$
$$px+\mathfrak{A},\ px+\mathfrak{B},\ px+\mathfrak{C},\ px+\mathfrak{D},...px+\mathfrak{L},$$

ita ut omnes numeri quadrati in priori classe contineantur, posterior vero classis naturae quadratorum prorsus adversetur.

19. Pro quolibet ergo divisore primo *p* his duabus classibus constitutis, $\frac{p-1}{2}$ quarum utraque species continet et quae ambae coniunctim omnes plane numeros continent exceptis multiplis ipsius *p,* quippe quorum iudicium est in promtu, omnes numeri in priori classe contenti hac gaudent proprietate, ut producta ex binis in eadem classe contineantur, in qua ergo simul non solum potestates singulorum quaecumque, sed etiam producta ex binis pluribusque harum potestatum occurrunt. Prior igitur classis, quam voco residuorum, numeris $\alpha,\ \beta,\ \gamma,\ \delta,...\lambda$ determinatur, dum altera classis, nonresiduorum, numeris $\mathfrak{A},\mathfrak{B},\mathfrak{C},\mathfrak{D},\ldots\mathfrak{L}$ definitur.

20. Demonstravi deinde etiam, si in classe residuorum occurrant duo numeri *r* et *rs,* quorum ille *r* huius *rs* sit factor, tum etiam huius alterum factorem in eadem classe reperiri. Cum enim dentur duo quadrata *aa* et *bb,* ut formae $aa-r$ et $bb-rs$ sint per numerum primum *p* divisibiles existentibus numeris *a* et *b* ipso *p* minoribus, etiam forma $aas-rs$ per *p* est divisibilis hincque etiam differentia $bb-aas$ et $(b+np)^2-aas$. Cum autem *a* et *b* sint ipso *p* minores, semper *n* ita assumere licet, ut fiat $b+np=ma.$ Ex quo talis forma *mmaa- aas* dabitur per *p* divisibilis adeoque et haec $mm-s$, ita ut sit $s=mm-np$ ac propterea numerus *s* inter residua reperiatur. Hinc sequitur, si *r* fuerit residuum, at *s* non-residuum, tum productum *rs* certe fore non-residuum; seu producta ex quovis residuo per non-residuum facta, veluti $\alpha\mathfrak{A},\alpha\mathfrak{B},\beta\mathfrak{A}$, inter non-residua reperiuntur.

21. Si igitur $\mathfrak{A}$ fuerit non-residuum, omnia haec producta $\alpha\mathfrak{A},\ \beta\mathfrak{A},\ \gamma\mathfrak{A},\ \delta\mathfrak{A},...\lambda\mathfrak{A}$ erunt non-residua; quae cum sint diversa inter se etiam reductione ad minimam formam facta eorumque numerus $\frac{p-1}{2}$, in iis adeo omnia non-residua continentur. Ex quo iam perspicuum est producta ex binis non-residuis, veluti $\alpha\beta\mathfrak{A}\mathfrak{A}$, ad classem residuorum esse referenda, quoniam $\alpha\beta$ est residuum et $\mathfrak{A}\mathfrak{A}$ utpote numerus quadratus per se inter residua occurrit. Simul vero patet producta ex ternis non-residuis, uti $\mathfrak{A}\mathfrak{B}\mathfrak{C}$, iterum in classem non-residuorum cadere, producta vero ex quaternis inter ipsa residua reperiri, et ita porro.

22. Praeterea vero etiam observo ex datis binis residuis α et β per divisionem novum residuum oriri et fractionem $\frac{\alpha}{\beta}$ inter residua esse referendam. Etsi enim fractiones ex hac ratione prorsus excluduntur, tamen, quia numerus α aequivalens censetur huic formae generali $\alpha + np$ universam speciem continenti, numerum utique ita accipere licet, ut $\frac{\alpha+np}{\beta}$ fiat numerus integer, de quo effatum est intelligendum, quod scilicet inter residua reperiatur. Hinc ergo omnes termini huius progressionis geometricae

$$\alpha,\ \beta,\ \frac{\beta^2}{\alpha},\ \frac{\beta^3}{\alpha^2},\ \frac{\beta^4}{\alpha^3},\ \text{etc.}$$

ex binis residuis α et β continuatae in classe residuorum continentur, si scilicet singuli ad formas integras revocentur. Quodsi enim fractio $\frac{\beta}{\alpha}$ aequivaleat numero integro *r,* statim sequentes numeri integri obtinentur

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\ \beta r^4\ \text{etc.},$$

qui ad minimam formam reducti non plures quam $\frac{p-1}{2}$ numeros diversos praebere possunt.

23. Consideremus ergo hanc progressionem geometricam

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\ \beta r^4\ \text{etc.},$$

et cum omnes termini diversi esse nequeant, praebeant hi termini βr^m et βr^{m+n} per p divisi idem residuum, ita ut differentia $\beta r^{m+n} - \beta r^m$ propterea $r^n - 1$ per p fiat divisibilis. Tum ergo etiam termini β et βr^n atque etiam α et βr^{n-1} ratione residui convenient; ex quo patet plura residua diversa prodire non posse, quam quae oriuntur ex his terminis initialibus

$$\alpha,\ \beta,\ \beta r,\ \beta r^2, \cdots \beta r^{n-2},$$

quoniam ex sequentibus βr^{n-1}, βr^n, βr^{n+1} etc. eadem residua eodem ordine recurrunt; quorum ergo residuorum, siquidem fuerint diversa, multitudo maior esse nequit quam $\frac{p-1}{2}$, quod evenit, si r^n sit minima potestas ipsius *r,* quae unitate minuta per p divisionem admittat. Hinc patet numerum n certe non superare $\frac{p-1}{2}$; ac si fuerit $n = \frac{p-1}{2}$, omnia plane residua obtinentur.

24. Sin autem ex terminis $\alpha,\ \beta,\ \beta r,\ \beta r^2,\cdots \beta r^{n-2},$ non omnia residua prodeant, sed quaedam omittantur, facile ostenditur ad minimum totidem omitti, quot adsunt. Si enim residuum γ inter ea non occurrat, quod etiam per $\alpha\delta$ repraesentare licet, quoniam $\gamma + mp$ semper ad formam $\alpha\delta$ revocari potest, tum etiam neque $\beta\delta$ neque $\beta\delta r$ neque $\beta\delta r^2$ etc. inter ea residua reperietur; quae cum sint diversa, excluso uno simul *n* excluduntur, unde *2n* numerum omnium $\frac{p-1}{2}$ superare nequit. Erit ergo vel $2n = \frac{p-1}{2}$ vel $2n < \frac{p-1}{2}$ et posteriori casu adhuc de novo ad minimum *n* residua excluduntur. Quare cum termini progressionis geometricae $\alpha,\ \beta,\ \beta r,\ \beta r^2,\cdots \beta r^{n-2},$ quorum numerus est *n,* vel omnia residua contineant ex quadratis orta, quorum multitudo est $= \frac{p-1}{2}$, vel inde exclusorum numerus sit $= n$ vel $= 2n$ vel $= 3n$ etc., evidens est numerum *n* necessario partem aliquotam ipsius $\frac{p-1}{2}$ esse debere ideoque minimum exponentem *n,* quo potestas r^n unitate minuta per *p* divisibilis reddatur, vel ipsi numero $\frac{p-1}{2}$ vel eiusdem parti cuipiam aliquotae esse aequalem.

25. Sive autem sit $n = \frac{p-1}{2}$, sive eius parti cuidam aliquotae aequetur, semper forma $r^{\frac{1}{2}(p-1)} - 1$ divisionem admittet per numerum primum *p.* Ponamus $p = 2q+1$, ut sit $\frac{p-1}{2} = q$; ac si ex binis quadratorum residuis quibuscumque α et β sumendo $r = \frac{\beta+np}{\alpha}$ formetur haec progressio geometrica

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\cdots \beta r^{q-2}$$

terminorum numero existente $= q,$ tum hinc vel omnia residua quadratorum $\alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\cdots \lambda$ resultabunt vel eorum tantum semissis vel pars tertia vel pars quarta aliave aliquota; simulque perspicitur, quot ab initio diversa prodierint, eadem deinceps eadem ordine continua repetitum iri. Semper autem termini sequentes $\beta r^{n-1},\ \beta r^n,\ \beta r^{n+1}$ etc. eadem residua reproducent $a,\ \beta,\ \beta r$ etc., quae initio habentur.

26. Quoties ergo *q* est numerus primus existente $p = 2q+1$, tum progressio geometrica ex binis quadratorum residuis quibusque α et β formata et ad *q* terminos continuata

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\cdots \beta r^{q-2}$$

omnium plane quadratorum residua exhibebit nullo neque excluso neque repetito. Omnia ergo reliqua residua $\gamma,\ \delta,\ \varepsilon,\cdots \lambda$ cum tali quopiam termino $\beta r^n,$ ut sit $n < q-1$, convenient. Sin autem numerus *q* fuerit compositus, puta $q = mn$ et $p = 2mn+1$, tum

evenire potest, ut non omnia residua quadratorum sic prodeant, sed tantum eiusmodi pars aliquota ipsius *q,* qualem eius indoles admittit. Quod si usu venit, tota progressio geometrica *q* terminis constans quasi sponte in duo plurave membra distinguitur, in quibus eadem residua recurrunt.

27. Cum sit $\frac{\beta}{\alpha} = r$ ideoque $\beta = \alpha r$, nostra progressio geometrica hoc modo expressa magis fit perspicua

$$\alpha,\ \alpha r,\ \alpha r^2,\ \alpha r^3, \cdots \alpha r^{q-1}$$

cuius omnes termini quia sunt per α multiplicati, hoc factore communi praetermisso progressio simplicius ita exhiberi potest. Proposito scilicet divisore prima $p = 2q+1$ si residuum quodcumque fuerit α, singuli termini huius progressionis geometricae quorum numerus est $= q$, inter residua quadratorum reperiuntur, ac si omnes ad diversas species pertineant, etiam universam residuorum classem implent. Fieri autem potest, uti vidimus, ut non omnia residua hoc modo prodeant, sed totius classis tantum pars aliquota, dum eadem post certam periodum iterum repetuntur, reliqua vero hinc prorsus excluduntur.

28. Sive autem omnia quadratorum residua ex hac progressione geometrica nascantur sive quaedam tantum pars aliquota, ea, quae terminis istius progressionis continentur, tam insignibus proprietatibus sunt praedita, ut operae omnino pretium sit eas accuratius evolvere. Primum igitur observo, si haec progressio geometrica ulterius continuetur, terminos sequentes α^q, α^{q+1}, α^{q+2} etc. aequivalere primis 1, α, α^2 etc., propterea quod a^{q-1} dividi certe potest per divisorum primum $p = 2q+1$. Adiecto ergo termino sequente a^q unitati aequivalente, ita ut habeamus

$$1,\ \alpha,\ \alpha^2,\ \alpha^3, \cdots \alpha^{q-3},\ \alpha^{q-2},\ \alpha^{q-1}, 1,$$

quia productum ex primo termino in ultimum est $= 1$, ex natura progressionis geometricae sequitur etiam producta ex secundo α in penultimum α^{q-1}, item ex tertio α^2 in antepenultimum α^{q-2} et in genere ex binis ab extremis aequidistantibus α^m et α^{q-m} ad unitatem reduci.

29. Dato ergo quocumque residuo α inter reliqua unum reperietur β, ita ut productum $\alpha\beta$ unitati aequivaleat seu sit $\beta = \frac{1+np}{\alpha}$, unde id facile invenitur. Quia igitur haec duo residua α et β tali vinculo inter se colligantur, ea *sociata* nominabo; ex quo superioris progressionis geometricae bini termini ab extremis aequidistantes huiusmodi bina residua sociata suppeditant. Terminus scilicet penultimus α^{q-1} aequivalet ipsi β^2, antepenultimus α^{q-2} ipsi β, et ita porro; unde si sociata subscribantur hoc modo

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\cdots\alpha^{q-3},\ \alpha^{q-2},\ \alpha^{q-1},\ 1,$$
$$1,\ \beta,\ \beta^2,\ \beta^3,\cdots\beta^{q-3},\ \beta^{q-2},\ \beta^{q-1},\ 1,$$

inferior series congruit cum superiori retro scripta. Semper autem residuum unitati associatum quoque est unitas.

30. Consideratio horum residuorum sociatorum aperit nobis viam ad insignes proprietates detegendas. Cum enim posito divisore primo $p = 2q+1$ sit numerus omnium residuorum *q,* quorum cuilibet praeter unitatem convenit suum sociatum, unitate exclusa reliqua, quorum numerus est $= q-1$, secundum hanc sociationem in paria distribui possunt binis sociatis invicem iungendis. Hinc si $q-1$ fuerit numerus impar ac propterea *q* par, necesse est, ut in hac distributione idem residuum, puta δ, bis occurrat. Verum idem residuum δ duobus diversis residuis associari nequit; si enim esset $\alpha\delta = 1$ et $\beta\delta = 1$, residua α et β non discreparent. Quare nihil aliud relinquitur, nisi ut idem residuum δ secum ipsum associetur sitque idcirco $\delta\delta = 1$, unde fit vel $\delta = 1$ vel $\delta = -1$; sed quia unitas iam est seposita, necesse est hoc casu, quo *q* est numerus par, inter residua reperiri -1 vel $p-1$.

31. En ergo egregiam demonstrationem veritatis supra iam observatae, quod, si divisor primus sit $p = 4m+1$ ideoque $q = 2m$, inter residua necessario occurrat -1 seu semper exhiberi queat quadratum *aa,* ut $aa+1$ per illum numerum primum $p = 4m+1$ dividi possit. Hinc simul patet, si inter residua sit numerus α, ibidem quoque productum $-1\cdot\alpha$, nempe $-\alpha$, occurrere hincque omnia residua ad minimam formam reducta tam positive quam negative adesse, omnino uti in exemplis § 14 allatis perspicitur. Simul vero etiam patet, si fuerit $p = 4m+3$ ideoque residuorum multitudo impar, ibi -1 locum habere non posse, quia tum singula residua utroque signo + et − occurrerent ideoque eorum numerus impar esse non posset. Ex quo sequitur per huiusmodi numerum primum $p = 4m+3$ nullam binorum quadratorum summam dividi posse.

32. Pro divisoribus autem primus formae $p = 4m+3$, si quadratum *aa* det residuum α, aliud semper dabitur quadratum *bb* praebens residuum $-\alpha$; sicque horum quadratorum summa $aa+bb$ per illum numerum primum erit divisibilis, ita ut nec *a* nec *b* superet 2*m*. Operae pretium ergo erit his casibus bina residua signo discrepantia iunctim exhibere simulque quadrata, unde nascuntur, adscribere.

$$p=5\begin{cases}1^2\\+1\\-1\\2^2\end{cases}\qquad p=13\begin{cases}1^2 & 2^2 & 4^2\\+1, & +4, & +3\\-1, & -4, & -3\\5^2 & 3^2 & 6^2\end{cases}\qquad p=17\begin{cases}1^2 & 6^2 & 2^2 & 5^2\\+1, & +2, & +4, & +8\\-1, & -2, & -4, & -8\\4^2 & 7^2 & 8^2 & 3^2\end{cases}$$

$$p=29\begin{cases}1^2 & 2^2 & 11^2 & 8^2 & 6^2 & 3^2 & 10^2\\+1, & +4, & +5, & +6 & +7, & +9, & +13,\\-1, & -4, & -5, & -6 & -7, & -9, & -13,\\12^2 & 5^2 & 13^2 & 9^2 & 14^2 & 7^2 & 4^2\end{cases}$$

$$p=37\begin{cases}1^2 & 15^2 & 2^2 & 9^2 & 3^2 & 11^2 & 14^2 & 7^2 & 4^2\\+1, & +3, & +4, & +7 & +9, & +10, & +11, & +12, & +16\\-1, & -3, & -4, & -7 & -9, & -10, & -11, & -12, & -16\\6^2 & 16^2 & 12^2 & 17^2 & 18^2 & 8^2 & 10^2 & 5^2 & 13^2\end{cases}$$

$$p=41\begin{cases}1^2 & 17^2 & 2^2 & 13^2 & 7^2 & 3^2 & 16^2 & 4^2 & 10^2 & 15^2\\+1, & +2, & +4, & +5 & +8, & +9, & +10, & +16, & +18, & +20\\-1, & -2, & -4, & -5 & -8, & -9, & -10, & -16, & -18, & -20\\9^2 & 11^2 & 18^2 & 6^2 & 19^2 & 14^2 & 20^2 & 5^2 & 8^2 & 12^2\end{cases}$$

33. Hinc evidens est pro divisore primo $p=4m+1$ tot modis, quot m continet unitates, bina quadrata radices limitem $2m$ non superantes habentia assignari posse, quorum summa sit divisibilis per numerum p. In his autem binis quadratis nulla lex, qua inter se cohaereant, perspicitur aliorumque summa modo maior reperitur modo minor ac minima quidem ubique ipsi numero p est aequalis. Num autem semper talis binorum quadratorum summa divisori p aequalis detur, hinc non facile demonstrari posse videtur. Cum autem ex alio fonte demonstraverim binorum quadratorum summam alios non admittere divisores, nisi qui ipsi sint binorum quadratorum summae, quoniam hic evictum est semper dari binorum quadratorum summas, quae sint per numerum primum $p = 4m + 1$ divisibiles, iam certo constat omnes numeros primos formae $4m+1$ esse summam duorum quadratorum. Praesens autem supplementum demonstrationem huius propositionis mirifice contrahit. Olim enim nonnisi per multas ambages ostendi dari semper eiusmodi binorum quadratorum summas, quae sint per quemlibet numerum primum formae $4m+1$ divisibiles, id quod hic in aprico est positum.

34. Data autem duorum quadratorum summa $aa+bb$ per numerum primum p divisibili alias inde binorum quadratorum summas idem praestantes facile reperire licet.

1. Si numeri *a* et *b* communem habeant divisorem, ut sit $a = nc$ et $b = nd$, etiam summa quadratorum $cc + dd$ per *p* erit divisibilis.

2. Si numeri *a* et *b* ambo sint impares ideoque $\frac{a+b}{2}$ et $\frac{a-b}{2}$ numeri integri, etiam horum quadratorum summa per *p* divisionem admittet; semissis autem ea est praecedentis.

3. Tum vero etiam hae quadratorum summae $(p-a)^2 + (p-b)^2$ vel $a^2 + (p-b)^2$ per *p* erunt divisibiles; unde si radices communem sortiantur divisorem, eo ad formam minorem redigi possunt.

4. Si ergo sint ambo impares $a = 2c+1$ et $b = 2d+1$, ob $p = 4m+1$ horum quadratorum summa $(2m-c)^2 + (2m-d)^2$ erit per *p* divisibilis; et si alter par $a = 2c$, alter impar $b = 2d+1$, haec summa $cc + (2m-d)^2$ erit per *p* divisibilis; hocque modo continuo plures huiusmodi binorum quadratorum summas invenire licet.

35. Exemplo haec fient clariora. Sumto igitur divisore $p = 41$ inventa sit summa duorum quadratorum $17^2 + 11^2$ per eum divisibilis, ut sit $a = 17$ et $b = 11$, atque per has regulas sequentes valores alii pro *a* et *b* reperientur

$$p = 41 \begin{cases} a = 17, 24 \,|\, 4, \;\; 4 \,|\, 1, 40 \,|\, 5 \\ b = 11, 30 \,|\, 5, 36 \,|\, 9, 32 \,|\, 4 \end{cases}$$

Tum vero porro ex casu, quo alteruter numerorum est $= 1$, alteri valor quicumque tribui alterque ita definiri potest, ut infra $\frac{1}{2}p$ subsistat. Scilicet invento casu $a = 1$ et $b = 9$ satisfacit quoque $a = m$ et $b = 9m$, ubi loco *b* sumi potest $9m - np$ seu $np - 9m$, ita ut *b* infra $\frac{1}{2}p$ deprimatur; sicque pro *a* omnes numeros accipere licebit

$a = 1$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	15	etc.
$b = 9$	18	14	5	4	13	19	10	1	8	17	15	6	3	12	20	etc.

Desideratur ergo methodus inter omnes hos binos valores litterarum *a* et *b* eos inveniendi, quorum quadratorum summa sit minima, ut deinceps demonstretur hanc summam ipsi divisori 41 certe fore aequalem; quod quidem praesenti casu evenit, si litterarum *a* et *b* valores sint 4 et 5.

36. Revertor autem ad eam residuorum ex quadratis oriundorum dispositionem, qua ea secundum progressionem geometricam disponi posse observavi. Sit igitur divisor primus $p = 2q+1$ et residua inde ex quadratis orta ordine quocumque scripta

$$1, \; \alpha, \; \beta, \; \gamma, \; \delta, \ldots \lambda,$$

quorum multitudo est $= q$, atque sequentes progressiones geometricae omnes in his residuis continebuntur :

$$1,\ \alpha,\ \alpha^2,\ \alpha^3, a^4, \cdots\ \alpha^{q-1}$$
$$1,\ \beta,\ \beta^2,\ \beta^3, \beta^4, \cdots\ \beta^{q-1}$$
$$1,\ \gamma,\ \gamma^2,\ \gamma^3, \gamma^4, \cdots\ \gamma^{q-1},$$
$$1,\ \delta,\ \delta^2,\ \delta^3, \delta^4, \cdots\ \delta^{q-1}$$
etc.,

in quibus omnibus termini sequentes $\alpha^q,\ \beta^q,\ \gamma^q,\ \delta^q, ...\lambda^q,$ unitati aequivalebunt, quippe qui omnes unitate minuti per divisorem p erunt divisibiles. Huiusmodi ergo progressiones geometricas tot exhibere licet, quot unitates in q continentur, in iisque omnibus nullus terminus occurret, qui non inter residua $1,\ \alpha,\ \beta,\ \gamma,\ \delta, ...\lambda,$ reperiatur.

37. Evenire autem potest, ut supra [§.24] est ostensum, ut non omnes istae progressiones geometricae, etiamsi cuiusque terminorum numerus sit $= q$, omnia residua praebeant, sed tantum eorum vel semissem vel trientem vel etiam quampiam partum aliquotam; quod quibus casibus contingat, accuratius est perpendendum.

Primum igitur observo, si q fuerit numerus primus, hoc nullo modo usu venire posse; si enim in huiusmodi progressione geometrica q terminorum non omnia residua occurrant, eorum, quae occurrunt, singula vel bis vel ter vel aliquoties occurrant necesse est. Unde si q est numerus primus, quaelibet progressio geometrica omnia residua diversa numero q complectitur. Ita si $p = 11$ et $q = 5$, ex quinque residuis

$$1,\ 4,\ -2,\ 5,\ 3$$

ab unitate incipiendo hae quatuor progressiones geometricae formantur

$$\left|\begin{array}{rl} & 1,\ 4,\ 4^2,\ 4^3,\ 4^4 \\ \text{seu} & 1,\ 4,\ 5,\ -2,\ 3 \end{array}\right| \left|\begin{array}{rl} & 1,\ -2,\ 2^2,\ -2^3,\ 2^4 \\ \text{seu} & 1,\ -2,\ 4,\ 3,\ 5 \end{array}\right|$$
$$\left|\begin{array}{rl} & 1,\ 5,\ 5^2,\ 5^3,\ 5^4 \\ \text{seu} & 1,\ 5,\ 3,\ 4,\ -2 \end{array}\right| \left|\begin{array}{rl} & 1,\ 3,\ 3^2,\ 3^2,\ 3^4 \\ \text{seu} & 1,\ 3,\ -2,\ 5,\ 4 \end{array}\right|$$

Ubi singula residua per omnia loca variantur praeter primum.

38. Hinc evidens est ex qualibet harum progressionum geometricarum reliquas facile formari posse, dum ex illa per saltum transiliendo vel unum vel duos vel plures terminos termini excerpuntur hac numeratione, cum ad finem fuerit perventum, iterum ab initio instituta. Ita si casum sumamus, quo $p = 23$ et $q = 11$ ac residua

$$1,\ 4,\ 9,\ -7,\ 2,\ -10,\ 3,\ -5,\ -11,\ 8,\ 6,$$

una progressione geometrica formata, cuius terminis indices inscribo, quo deinceps reliquae terminis per saltum excerpendis facilius exhiberi queant, decem progressiones geometricae ita se habebunt:

												Seq.
1.	Indices	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10	0
	Progressio	1,	4,	−7,	−5,	3,	−11,	2,	8,	9,	−10,	6	1
2.	Indices	0,	2,	4,	6,	8,	10,	1,	3,	5,	7,	9	0
	Progressio	1,	−7,	3,	2,	9,	6,	4,	−5,	−11,	8,	−10	1
3.	Indices	0,	3,	6,	9,	1,	4,	7,	10,	2,	5,	8	0
	Progressio	1,	−5,	2,	−10,	4,	3,	8,	6,	−7,	−11,	9	1
4.	Indices	0,	4,	8,	1,	5,	9,	2,	6,	10,	3,	7	0
	Progressio	1,	3,	9,	4,	−11,	−10,	−7,	2,	6,	−5,	8	1
5.	Indices	0,	5,	10,	4,	9,	3,	8,	2,	7,	1,	6	0
	Progressio	1,	−11,	6,	3,	−10,	−5,	9,	−7,	8,	4,	2	1
6.	Indices	0,	6,	1,	7,	2,	8,	3,	9,	4,	10,	5	0
	Progressio	1,	2,	4,	8,	−7,	9,	−5,	−10,	3,	6,	−11	1
7.	Indices	0,	7,	3,	10,	6,	2,	9,	5,	1,	8,	4	0
	Progressio	1,	8,	−5,	6,	2,	−7,	−10,	−11,	4,	9,	3	1
8.	Indices	0,	8,	5,	2,	10,	7,	4,	1,	9,	6,	3	0
	Progressio	1,	9,	−11,	−7,	6,	8,	3,	4,	−10,	2,	−5	1
9.	Indices	0,	9,	7,	5,	3,	1,	10,	8,	6,	4,	2	0
	Progressio	1,	−10,	8,	−11,	−5,	4,	6,	9,	2,	3,	−7	1
10.	Indices	0,	10,	9,	8,	7,	6,	5,	4,	3,	3,	1	0
	Progressio	1,	6	−10,	9,	8,	2,	−11,	3,	−5,	−7,	4	1

Indices scilicet hic ultra 11 ascensuri subtrahendo 11 sunt depressi. Hic porro observari convenit bina residua, quorum indices iuncti faciunt 11 seu in genere q, esse inter se sociata eorumque productum unitati aequivalere. Hoc nempe casu residua sociata sunt

$$\begin{array}{cccccc} 4, & -7, & -5, & 3, & -11, \\ 6, & -10, & 9, & 8, & 2. \end{array}$$

39. Consideremus nunc quoque casus, quibus q est numerus compositus ac primo quidem duplus cuiuspiam numeri primi. Ab exemplo exordiamur, quo $p = 13$ et $q = 6 = 2 \cdot 3$ ac residua haec

$$1,\ 4,-4,\ 3,-1,-3,$$

unde hae quinque progressiones geometricae formentur

$$\begin{aligned}
&\text{I. } 1, \quad 4, \quad 3, \ -1, \ -4, \ -3,\\
&\text{II. } 1, \ -4, \quad 3, \quad 1, \ -4, \quad 3,\\
&\text{III. } 1, \quad 3, \ -4, \quad 1, \quad 3, \ -4,\\
&\text{IV. } 1, \ -1, \quad 1, \ -1, \quad 1, \ -1,\\
&\text{V. } \ 1, \ -3, \ -4, \ -1, \quad 3, \quad 4.
\end{aligned}$$

Ubi prima et quinta omnia continent residua, secunda vero et tertia eorum tantum semissem 1, - 4, 3, quae bis repetuntur reliquis $-1,\ +4,\ -3$ exclusis, quarta vero duo tantum habet $+1$ et -1 ter repetita.

Similis ratio deprehenditur in casu $p = 29$ et $q = 14 = 2 \cdot 7$, quo residua sunt

$$1,\ 1,\ 4,\ 4,\ 5,\ 5,\ 6,\ 6,\ 7,-7,\ 9,-9,\ 13,-13,$$

unde hae progressiones geometricae formantur

I.	1,	-1	1,	-1,	1,	-1	1,	-1,	1,	-1,	1,	-1,	1,	-1,
II.	1,	4,	-13,	6,	-5,	9,	7,	-1,	-4,	13,	-6,	5,	-9,	7,
III.	1,	-4	-13,	-6,	-5,	-9,	7,	1,	-4,	-13	-6,	-5,	-9,	7,
IV.	1,	5,	-4,	9,	-13,	-7,	-6,	-1,	-5,	4,	-9,	13,	7,	6,
V.	1,	-5,	-4,	-9,	-13,	7,	-6,	1,	-5,	-4,	-9,	-13,	7,	-6,
VI.	1,	6,	7,	13,	-9,	4,	-5,	-1,	-6,	-7,	-13,	9,	-4,	5,
VII.	1,	-6,	7,	-13,	-9,	-4,	-5,	1,	-6,	7,	-13,	-9,	-4,	-5,
VIII.	1,	7,	-9,	-5,	-6,	-13,	-4,	1,	7,	-9,	-5,	-6,	-13,	-4,
IX.	1,	-7,	-9,	5,	-6,	13,	-4,	-1,	7,	9,	-5,	6,	-13,	4,
X.	1,	9,	-6,	4,	7,	5,	-13,	-1,	-9,	6,	-4,	-7,	-5,	13,
X.	1,	-9,	-6,	-4,	7,	-5,	-13,	1,	-9,	-6,	-4,	7,	-5,	-13,
XI.	1,	13,	-5,	-7,	-4,	6,	-9,	-1,	-13,	5,	7,	4,	-6,	9,
XIII.	1,	-13,	-5,	7,	-4,	-6,	-9,	1,	-13,	-5,	7,	-4,	-6,	-9.

40. Antequam hinc quicquam concludimus, evolvamus etiam casum, quo q est productum ex aliis binis numeris primis. Sit ergo divisor $p = 31$ et $q = 15 = 3 \cdot 5$, quo casu residua sunt

1, 4, 9, –15, –6, 5, –13, 2, –12, 7, 3, 11, 14, 10, 8,

unde sequentes progressiones geometricae formantur, ubi quidem cuique suam sociatam retro dispositam adiungo,

I.	1,	4	-15,	2,	8,	1	4,	-15,	2,	8,	1,	4,	-15,	2	8,
II.	1,	8,	2,	-15,	4,	1,	8,	2,	-15,	4,	1,	8,	2,	-15	4,
III.	1,	9,	-12,	-15,	-11,	-6,	8,	10,	-3,	4	5,	14,	2,	-13,	7,
IV.	1,	7,	-13,	2,	14,	5,	4,	-3,	10,	8,	-6,	-11,	-15,	-12,	9,
V.	1,	2,	4,	8,	-15,	1,	2,	4,	8,	-15,	1,	2,	4,	8,	-15,
VI.	1,	-15,	8,	4,	2,	1,	-15,	8,	4,	2,	1,	-15,	8,	4,	2,
VII.	1,	-3,	9,	4,	-12,	5,	-15,	14,	-11,	2,	-6,	-13,	8,	7,	10,
VIII.	1,	10,	7,	8,	-13,	-6,	2,	-11,	14,	-15,	5,	-12,	4,	9,	-3,
IX.	1,	5,	-6,	1,	5,	-6,	1,	5,	-6,	1,	-5,	-6,	1,	5,	-6,
X.	1,	-6,	5,	1,	-6,	5,	1,	-6,	5,	1,	-6,	5,	1,	-6,	5,
XI.	1,	-11,	-3,	2,	9,	-6,	4,	-13,	-12,	8,	5,	7,	-15,	10,	14,
XII.	1,	14,	10,	-15,	7,	5,	8,	-12,	-13,	4,	-6,	9,	2,	-3,	-11,
XIII.	1,	-12,	-11,	8,	-3,	5,	2,	7,	9,	-15,	-6,	10,	4,	14,	-13,
XIV.	1,	-13,	-14,	4,	10,	-6,	-15,	9,	7,	2,	5,	-3,	8,	-11,	-12.

41. Has progressiones geometricas intuenti mox patet earum alias esse completas, quarum termini omnia residua exhibeant, alias vero esse periodicas, quae scilicet duabus pluribusve periodis constent, in quibus eadem residua eodem ordine recurrant, quam distinctionem inter progressiones completas et periodicas probe notasse iuvabit. Periodicae scilicet locum inveniunt, quando posito divisore primo $p = 2q+1$ numerus q in duos factores est resolubilis, ut sit $q = mn$; tum enim eiusmodi progressiones geometricae dabuntur, quae continent m periodos qualibet n residua complectente; ac tales quidem assignari poterunt tot, quot numerus $n-1$ continet unitates. Cum enim in eadem periodo cuiusque termini omnes potestates occurrant, evidens est quemque pro denominatore sumtum similem progressionem periodicam producere, nisi forte periodorum numerus adeo duplicetur vel multiplicetur, hoc est in duas pluresve periodos subdividatur.

42. Ex progressione autem completa, quaecumque ea sit, facile reliquae omnes, sive sint completae sive periodicae, formantur. Sit enim divisor primus $p = 2q+1$ haecque progressio completa

indices 0, 1, 2, 3, 4, 5, $\cdots\cdots q-1$,

progressio 1, α, α^2, α^3, a^4, $a^5, \cdots\cdots \alpha^{q-1}$;

si hinc excerpantur per saltus aequales termini

$$0,\ n,\quad 2n,\quad 3n,\quad 4n,\cdots nq-n,$$
$$1,\ \alpha^n,\ \alpha^{2n},\alpha^{3n},\ \alpha^{4n},\ \cdots\alpha^{nq-n},$$

haec progressio erit completa, si numerus *n* ad *q* fuerit primus; sin autem *n* et *q* habeant communem divisorem, puta *d,* tum haec progressio totidem habebit periodos, in quarum singulis eadem residua numero $\frac{q}{d}$ recurrent, reliqua autem inde prorsus excludentur. Numerus autem harum periodorum maximo communi divisore inter *n* et *q* definietur. At vero vicissim ex progressione periodica non licet progressionem completam formare.

43. Imprimis autem hic notari meretur in omnibus his progressionibus summam omnium terminorum semper esse nihilo aequalem seu per divisorem *p* divisibilem, quod hoc modo demonstratur. Cum a^q-1 per *p* divisionem admittat, haec autem forma in factores resolvatur

$$\alpha-1 \text{ et } 1+\alpha+\alpha^2+\alpha^3+\ \cdots+\alpha^{q-1},$$

quorum ille $\alpha-1$ certe non per *p* est divisibilis, necesse est hunc alterum, hoc est summam totius nostrae progressionis, per numerum *p* divisionem admittere. Ac si progressio habeat periodos, termini cuiusque periodi iunctim sumti seu summa omnium residuorum inde oriundorum per *p* erit divisibilis, id quod in exemplis supra allatis per se est manifestum.

44. Ex eodem autem fonte colligitur, si progressio geometrica fuerit completa et *q* habeat factorem *tn,* ut sit $q=mn$ et divisor primus $p=2mn+1$, tum ob formam $\alpha^{mn}-1$ divisibilem per α^m-1, quae per *p* divisibilis non existit, quia progressio alioquin completa non foret, quotum inde ortum

$$1+\alpha^m+\alpha^{2m}+\alpha^{3m}+\ \cdots+\alpha^{(n-1)m}$$

per divisorem *p* fore divisibilem. Quamobrem si tota progressio *m* membra distribuatur hoc modo

$$1,\ \alpha,\ \cdots\ \alpha^{m-1}\ \big|\ \alpha^m,\ \alpha^{m+1},\cdots\ \alpha^{2m-1}\ \big|\ \alpha^{2m},\ \alpha^{2m+1},\cdots\ \alpha^{3m-1}\ \big|\ \cdots\ \alpha^{(n-1)m},\cdots\ \alpha^{mn-1},$$

quorum membrorum numerus est *n,* haecque membra ita sibi subscribantur

1	α,	α^2,	$\cdots\alpha^{m-1}$,
α^m,	α^{m+1},	α^{m+2},	$\cdots\ \alpha^{2m-1}$,
α^{2m}	α^{2m+1},	α^{2m+2},	$\cdots\ \alpha^{3m-1}$,
..	..	..	..
..	..	..	..

$$\alpha^{(n-1)m} \mid \alpha^{(n-1)m+1} \mid \alpha^{(n-1)m+2} \mid \cdots\ \alpha^{nm-1},$$

tum summae terminorum in qualibet columna verticali positorum ad nihilum reducentur seu per divisorem primum $p = 2mn+1$ divisibiles erunt. Tot autem diversis modis progressio completa in huiusmodi membra distribui potest, quot numerus *q* habuerit divisores.

45. Prima autem columna verticalis simul dabit periodos pro omnibus progressionibus periodicis. De his numeris tenendum est eos non solum esse residua quadratorum, sed etiam altiorum potestatum parium. Scilicet si divisor primus sit huius formae $p = 2mn+1$, quemadmodum inter numeros ipso minores, quorum multitudo est $= 2mn$, tantum semissis *mn* in residuis quadratorum occurrit totidemque inde excluduntur, ita potestates exponentis *2m* per eundem numerum *p* dividendo tantum *n* diversa residua inde resultant et reliqui omnes, quorum multitudo est $(2m-1)n$, ita sunt comparati, ut in forma $a^{2m} - ip$ nullo modo contineantur seu nulla exhiberi possit potestas exponentis *2m,* quae ullo istorum numerorum minuta per numerum primum $p = 2mn+1$ fiat divisibilis.

46. Neque vero haec proprietas ad potestates exponentium parium est adstricta, sed in genere pronunciare licet, si divisor primus sit formae $p = mn+1$, qui scilicet unitate minutus In factores *m* et *n* resolvi possit, ac potestates exponentis *m,* nempe

$$1,\ 2^m,\ 3^m,\ 4^m,\ 5^m,\ 6^m, \cdots (p-1)^m,$$

per eum dividantur, tum inter residua tantum *n* diversos numeros occurrere, quorum singuli *m* vicibus repetantur, reliqui autem numeri omnes, quorum multitudo est $(m-1)n$, hinc excludantur; ex quo insignes proprietates numerorum, qui sunt potestates, ratione divisibilitatis per numeros primos agnoscere licet.

47. Quoniam igitur nullum est dubium, quin hinc multae praeclarae numerorum proprietates erui queant, exempla plurium numerorum primorum hic adiicere visum est pro iisque residua, quae ex divisione potestatum nascuntur, exhibere, ubi quidem sociata iunctim repraesentantur:

l. Divisor $p = 3 = 2+1$

Potestates Residuum

a^2 {1

2. Divisor $p = 5 = 2\cdot 2+1$

Potestates Residuum

a^2 {1, −1

a^4 {1,

3. Divisor $p = 7 = 2\cdot 3+1$

Potestates Residuum

a^2 {1, 2, −3

a^3 {1, −1

a^6 {1

4. Divisor $p = 11 = 2\cdot 5+1$

Potestates Residuum

a^2 {1, 4, 5, 3, −2

a^5 {1, −1

a^{10} {1

5. Divisor $p = 13 = 2\cdot 2\cdot 3+1$

Potestates Residuum

a^2 {1, 4, 3, −1, −3, −4

a^3 {1, −5, −1, 5

a^4 {1, 3, −4

a^6 {1, −1

a^{12} {1

6. Divisor $p = 17 = 2^4+1$

Potestates Residuum

a^2 {1, 2, 4, 8, −1, −8, −4, −2

a^4 {1, 4, −1, −4

a^8 {1, −1

a^{16} {1

7. Divisor $p = 19 = 2\cdot 3\cdot 3+1$

Potestates Residuum

a^2 {1, 4, −3, 7, 9, 5, 6, −8, −2

a^3 {1, 8, 7, −1, −7, −8

a^6 {1, 7, −8

a^9 {1, −1

8. Divisor $p = 23 = 2\cdot 11+1$

Potestates Residuum

a^2 {1, 4, −7, −5, 3, −11, 6, −10, 9, 8, 2

a^{11} {1, −1

9. Divisor $p = 29 = 2 \cdot 2 \cdot 7 + 1$

Potestates Residuum

a^2	$\begin{cases} 1, & 4, & -13, & 6, & -5, & 9, & 7, & -1 \\ & -7, & -9, & 5, & -6, & 13, & -4 \end{cases}$
a^4	$\begin{cases} 1, & -13, & -5, & 7 \\ & -9, & -6, & -4 \end{cases}$
a^7	$\begin{cases} 1, & 12, & -1 \\ & -12 \end{cases}$
a^{14}	$\{1, \quad -1$

10. Divisor $p = 31 = 2 \cdot 3 \cdot 5 + 1$

Potestates Residuum

a^2	$\begin{cases} 1, & 9, & -12, & -15, & -11, & -6, & 8, & 10 \\ & 7, & -13, & 2, & 14, & 5, & -4, & -3 \end{cases}$
a^3	$\begin{cases} 1, & -4, & -15, & -2, & 8, & -1 \\ & -8, & 2, & 15, & 4 \end{cases}$
a^5	$\begin{cases} 1, & -5, & -6, & -1 \\ & 6, & 5 \end{cases}$
a^6	$\begin{cases} 1, & 2, & 4 \\ & -15, & 8 \end{cases}$
a^{10}	$\{1, \quad 5$
a^{15}	$\{1, \quad -1$

11. Divisor $p = 37 = 2\cdot 2\cdot 3\cdot 5+1$

Potestates	Residuum
a^2	$\begin{cases} 1, & 4, & 16, & -10, & -3, & -12, & -11, & -7, & 9, & -1 \\ & -9, & 7, & 11, & 12, & 3, & 10, & -16, & -4 \end{cases}$
a^3	$\begin{cases} 1, & 8, & -10, & -6, & -11, & -14, & -1 \\ & 14, & 11, & 6, & 10, & -8 \end{cases}$
a^4	$\begin{cases} 1, & 16, & -3, & -11, & 9 \\ & 7, & 12, & 10, & -4 \end{cases}$
a^6	$\begin{cases} 1, & -10, & -11, & -1 \\ & 11, & 10 \end{cases}$
a^9	$\begin{cases} 1, & -6, & -1 \\ & 6 \end{cases}$
a^{12}	$\begin{cases} 1, & -11 \\ & 10 \end{cases}$
a^{18}	$\{1, \quad -1$

12. Divisor $p = 41 = 2^3\cdot 5+1$

Potestates	Residuum
a^2	$\begin{cases} 1, & -2, & 4, & -8, & 16, & 9, & -18, & -5, & 10, & -20, & -1 \\ & 20, & -10, & 5, & 18, & -9, & -16, & 8, & -4 & 2 \end{cases}$
a^4	$\begin{cases} 1, & 4, & 16, & -18, & 10, & -1 \\ & -10, & 18, & -16, & -4 \end{cases}$
a^5	$\begin{cases} 1, & -3, & 9, & 14, & -1 \\ & -14, & -9, & 3 \end{cases}$
a^8	$\begin{cases} 1, & 16, & 10 \\ & 18, & -4 \end{cases}$
a^{10}	$\begin{cases} 1, & 9, & -1 \\ & -9 \end{cases}$
a^{20}	$\{1, \quad -1$

13. Divisor $p = 43 = 2 \cdot 3 \cdot 7 + 1$

Potestates	Residuum
a^2	$\begin{cases} 1, & 9, & -5, & -2, & -18, & 10, & 4, & -7, & -20, & -8, & 14 \\ -19, & 17, & 21, & -12, & 13, & 11, & 6, & 15, & 16, & -3 \end{cases}$
a^3	$\begin{cases} 1, & 8, & 21, & -4, & 11, & 2, & 16, & -1 \\ -16, & -2, & -11, & 4, & -21, & -8 \end{cases}$
a^6	$\begin{cases} 1, & 21, & 11, & 16 \\ -2, & 4, & -8 \end{cases}$
a^7	$\begin{cases} 1, & 6, & -7, & -1 \\ 7, & 6 \end{cases}$
a^{14}	$\begin{cases} 1, & -7 \\ 6 \end{cases}$
a^{21}	$\{1, \quad -1$

14. Divisor $p = 47 = 2 \cdot 23 + 1$

Potestates	Residuum
a^2	$\begin{cases} 1, & 4, & 16, & 17, & 21, & -10, & 7, & -19, & 18, & -22, & 6, & -23 \\ 12, & 3, & -11, & 9, & 14, & -20, & -5, & -13, & -15, & 8, & 2 \end{cases}$
a^{23}	$\{1, \ -1$

15. Divisor $p = 53 = 2 \cdot 2 \cdot 13 + 1$

Potestates	Residuum
a^2	$\begin{cases} 1, & 4, & 16, & 11, & -9, & 17, & 15, & -7, & -25, & 6, & 24, & -10, & 13, & -1 \\ -13, & 10, & -24, & -6, & 25, & -7, & -15, & -17, & 9, & -11, & -16, & -4 \end{cases}$
a^4	$\begin{cases} 1, & 16, & -9, & 15, & -25, & 24, & 13 \\ 10, & -6, & -7, & -17, & -11, & -4 \end{cases}$
a^{13}	$\begin{cases} 1 & -23, & -1 \\ 23 \end{cases}$
a^{26}	$\{1, \ -1$

16. Divisor $p = 59 = 2 \cdot 29 + 1$

Potestates	Residuum
a^2	$\begin{cases} 1, & 4, & 16, & 5, & 20, & 21, & 25, & -18, & -13, & 7, & 28, & -6, & -24, & 2 \\ 15, & -11, & 12, & 3, & -14, & 26, & -23, & 9, & 17, & 19, & -10, & 27, & -8 \end{cases}$
a^{29}	$\{1, \ -1$

17. Divisor $p = 61 = 2\cdot 2\cdot 3\cdot 5 + 1$

Potestates	Residuum
a^2	$\left\{\begin{array}{l} 1,\ 4,\ 16,\ 3,\ 12,\ -13,\ 9,\ -25,\ 22,\ 27,\ -14,\ 5,\ -20,\ 19,\ 15, \\ -15,\ -19,\ -20,\ -5,\ 14,\ -27,\ -22,\ 25,\ -9,\ 13,\ -12,\ -3,\ -16,\ -4 \end{array}\right.$
a^3	$\left\{\begin{array}{l} 1,\ 8,\ 3,\ 24,\ 9,\ 11,\ 27,\ -28,\ 20,\ -23,\ -1 \\ 23,\ -20,\ 28,\ -27,\ -11,\ -9,\ -24,\ -3,\ -8 \end{array}\right.$
a^4	$\left\{\begin{array}{l} 1,\ 16,\ 12,\ 9,\ 22,\ -14,\ 20,\ 15 \\ -19,\ -5,\ -27,\ 25,\ 13,\ -3,\ -4 \end{array}\right.$
a^5	$\left\{\begin{array}{l} 1,\ -29,\ -13,\ 11,\ -14,\ -21,\ 15 \\ 21,\ 14,\ -11,\ 13,\ 29,\ -1 \end{array}\right.$
a^6	$\left\{\begin{array}{l} 1,\ 3,\ 9,\ 27,\ 20,\ -1 \\ -20,\ -27,\ -9,\ -3 \end{array}\right.$
a^{10}	$\left\{\begin{array}{l} 1,\ -13,\ -14,\ -1 \\ 14,\ 13 \end{array}\right.$
a^{12}	$\left\{\begin{array}{l} 1,\ -3,\ 9,\ -1 \\ 20,\ -27 \end{array}\right.$
a^{15}	$\left\{\begin{array}{l} 1,\ 11,\ -1 \\ -11, \end{array}\right.$
a^{20}	$\left\{\begin{array}{l} 1, -14 \\ 13, \end{array}\right.$
a^{30}	$\{1, -1$

CONCLUSIO

DE POTESTATIBUS CUIUSQUE ORDINIS ET RESIDUIS IN EARUM DIVISIONE PER NUMEROS PRIMOS RELICTI

48. Quemadmodum in his exemplis residua pro singulis potestatibus per progressiones geometricas sunt exhibita, quae simul retro continuatae bina residua sociata iunctim repraesentant, ita idem pro potestatibus primi ordinis fieri potest, ubi quidem omnes plane numeri divisore minores occurrere debent, ita ut, si divisor primus sit $p = 2q + 1$, multitudo residuorum diversorum sit $= 2q$, quae ad minimam formam reducta erunt $\pm 1,\ \pm 2,\ \pm 3,\ \pm 4$ etc. usque ad $\pm q$. Hac vero residua omnia quoque secundum progressionem geometricam disponi possunt ab unitate incipientem, dummodo pro eius denominatore seu secundo termino eiusmodi numerus accipiatur, qui omnes plane numeros producat, quod evenit, si is ita fuerit comparatus, ut nulla eius potestas, cuius exponens minor sit quam $2q$, pro residuo unitatem relinquat. Tales autem numeros pro

quovis divisore dari certum est, etiamsi eos assignare maxime difficile videatur eorumque indoles ad profundissima numerorum mysteria sit referenda.

49. Sit igitur in genere pro divisore primo $p = 2q+1$ littera *a* eiusmodi numerus, cuius potestates per *p* divisae omnes numeros ipso *p* minores pro residuis relinquant neque in serie geometrica

$$1,\ a,\ a^2,\ a^3,\ a^4 \text{ etc.}$$

unitas ante recurrat, quam ad potestatem a^{2q} fuerit perventum, quippe quae semper per $p = 2q+1$ divisa unitatem relinquit, sicque omnes potestates hac minores diversa residua producant. Cum igitur potestas a^q non relinquat unitatem et $a^{2q}-1 = (a^q+1)(a^q-1)$ erit a^q+1 per *p* divisibilis et potestas a^q residuum dabit -1; tum vero sequentes potestates a^{q+1}, a^{q+2}, a^{q+3}, etc.. dabunt residua $-a, -a^2, -a^3$ etc., quae ita sunt comparata, ut cum antecedentibus a^{q-1}, a^{q-2}, a^{q-3}, etc. ordine iuncta bina residua sociata exhibeant, quorum scilicet productum a^{2q} unitati aequivaleat. Sequenti ergo modo haec residua per associationem repraesentare poterimus:

Indices	0,	1,	2 ,	3,	4,	$q-3$,	$q-2$,	$q-1$,	q
	1,	a^1,	a^2,	a^3,	a^4, ….	a^{q-3},	a^{q-2},	a^{q-1},	-1,
		$-a^{q-1}$,	$-a^{q-2}$,	$-a^{q-3}$,	$-a^{q-4}$, ...	$-a^3$,	$-a^2$,	$-a$	
indices	$2q$,	$2q-1$,	$2q-2$,	$2q-3$,	$2q-4$,	$q+3$,	$q+2$,	$q+1$,	q

ubi bina residua sibi subscripta sunt inter se sociata, extrema vero $+1$ et -1 solitaria, quippe quae secum ipsa sociantur.

50. Tali progressione geometrica constituta, quae omnia residua ex potestatibus primi ordinis oriunda, hoc est omnes plane numeros, complectitur, ex ea omnia residua pro potestatibus cuiusvis ordinis innotescent, eodem scilicet divisore primo $p = 2q+1$ retento.

Residua nimirum ex divisione quadratorum orta erunt

$$1,\ a^2,\ a^4,\ a^6,\ a^8\ \cdots a^{2q-2},$$

quae indicibus tantum paribus respondent et ita per associationem exhibentur

$$\begin{matrix} 1, & a^2, & a^4, & a^6, & a^8 & \text{etc.} \\ & -a^{q-2}, & -a^{q-4}, & -a^{q-6}, & -a^{q-8} & \text{etc.} \end{matrix}$$

in quibus ergo -1 reperietur, si q fuerit numerus par.

Pro cubis autem eos tantum terminos accipi oportet, quorum indices sunt multipla ternarii,

$$1,\ a^3,\ a^6,\ a^9 \text{ etc.}$$

Unde patet, si exponens $2q$ divisionem per 3 admittat, multitudinem residuorum ad trientem redigi, dum reliquis casibus omnia plane residua occurrunt.

Simili modo residua potestatum quartarum obtinentur ex indicibus per 4 divisibilibus seu ex his potestatibus

$$1,\ a^4,\ a^8,\ a^{12} \text{ etc.}$$

et residua potestatum quintarum ex his

$$1,\ a^5,\ a^{10},\ a^{15} \text{ etc.}$$

51. Tantum ergo opus est, ut pro quolibet divisore prima $p = 2q+1$ idonei numeri pro a habeantur, ex cuius potestatibus omnia plane residua resultent; ad quod autem nullam certam regulam mihi esse cognitam fateri cogor. Hoc saltem observasse iuvabit, si unus huiusmodi numerus a fuerit cognitus, eius socium, qui sit b, ut $ab-1$ per p fiat divisibile, quoque pari proprietate esse praeditum; vidimus autem hunc socium b vel per a^{2q-1} vel per $-a^{q-1}$ exhiberi posse. Ex quo concludere licet tum etiam pro a quamvis eius potestatem a^n, cuius exponens n sit ad numerum $2q$ primus, accipi posse, ubi quidem sufficit pro n numeros ipso $2q$ minores assumsisse, cum ex altioribus potestatibus eadem residua repetantur. Quoniam vero certa lex adhuc latet, pro divisoribus simplicioribus idoneos numeros pro a assumendos, ex cuius scilicet potestatibus omnia plane residua nascantur, exhibebo:

Divisores primi	Numeri pro a assumendi
$p=3,\ q=1$	-1
$p=5, q=2$	± 2
$p=7, q=3$	$-2,\ +3$
$p=11,\ q=5$	$+2, -3,\ -4, -5$
$p=13,\ q=6$	$\pm 2,\ \pm 6$
$p=17,\ q=8$	$\pm 3,\ \pm 5,\ \pm 6,\ \pm 7$
$p=19, q=9$	$+2, +3,\ -4,\ -5,\ -6,\ -9$
$p=23,\ q=11$	$-2,\ -3,\ -4,\ +5,\ -6,\ +7,\ -8,\ -9,\ +10,\ +11$
$p=29,\ q=14$	$\pm 2,\ \pm 3,\ \pm 8,\ \pm 10,\ \pm 11,\ \pm 14$

$p=31,\ q=15$	$+3,\ -7,\ -9,\ -10,\ +11,\ +12,\ +13,\ -14$
$p=37, q=18$	$\pm2,\ \pm5,\ \pm13,\ \pm15,\ \pm17,\ \pm18$
$p=41, q=20$	$\pm6,\ \pm7,\ \pm11,\ \pm12,\ \pm13,\ \pm15,\ \pm17,\ \pm19$

52. In casu postremo $p=41$ ergo patet pro *a* minorem numerum quam 6 assumi non posse, cum in praecedentibus progressio geometrica ex minoribus numeris formari queat; unde pro hoc divisore $p=41$ ista progressio geometrica ita se habebit:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1,	$+6,-5,+11,-16,-14,-2,-12,+10,+19,-9,-13,+4,-17,-20,+3,+18,-15,-8,-7$																			-1
	$+7,+8,+15,-18,-3,+20,+17,-4,+13,+9,-19,-10,+12,+2,+14,+16,-11,+5,-6$																			

Hinc si ii numeri excerpantur, qui indicibus paribus respondent, habebuntur residua ex quadratis orta; sin autem ii excerpantur, qui indicibus vel per 4 vel 5 vel 8 vel 10 vel 20 divisibilibus conveniunt, residua pro eiusdem nominis potestatibus obtinebuntur, eaque ipsa, quae iam supra [§ 47] sunt recensita. Similisque est ratio omnium reliquorum numerorum primorum.

53. Quod autem ad multitudinem horum numerorum *a* attinet, observo eam quovis casu $p=2q+1$ aequalem esse multitudini eorum numerorum ipso *p* minorum, qui sint ad $2q$ primi; atque alio loco ostendi ad hanc multitudinem inveniendam numerum $2q$ in factores suos primos resolvi debere, ita ut, si fuerit

$$2q = f^{\zeta} g^{\eta} h^{\theta} k^{\chi},$$

sit ista multitudo

$$= (f-1)^{\zeta} (g-1)^{\eta} (h-1)^{\theta} (k-1)^{\chi}.$$

Definita autum pro quovis numero $p=2q+1$ hac multitudine sint ipsi numeri ad $2q$ primi $1,\ \alpha,\ \beta,\ \gamma,\ \delta$ etc., atque si datus fuerit unus numerus *a* quicumque, reliqui ideoque omnes erunt

$$a,\ a^{\alpha}-np,\ a^{\beta}-np,\ a^{\gamma}-np,\ a^{\delta}-np,\ \text{etc.}$$

sumendo *n* ita, ut omnes isti numeri infra *p* deprimantur. Haec fortasse consideratio viam aperiet pro quovis casu hos numeros investigandi.